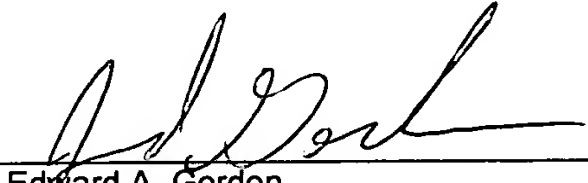
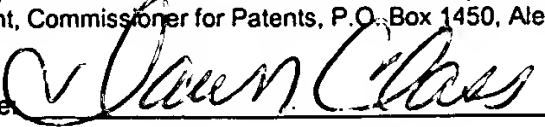
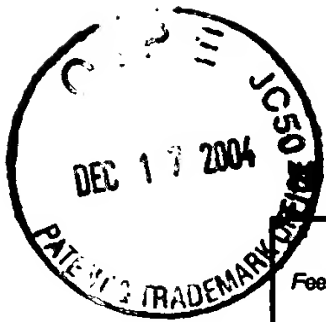


12-20-04

AF/2141 #
LZW

TRANSMITTAL OF APPEAL BRIEF			Docket No. BBNT-P01-109
In re Application of: Donaghey et al.			
Application No. 09/658207	Filing Date September 8, 2000	Examiner L. H. Luu	Group Art Unit 2141
Invention: SYSTEM AND METHOD FOR SELECTING AND DISSEMINATING POLICIES			
<p style="text-align: center;"><u>TO THE COMMISSIONER OF PATENTS:</u></p> <p>Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: <u>October 18, 2004</u>.</p> <p>The fee for filing this Appeal Brief is <u>\$ 500.00</u>.</p> <p><input checked="" type="checkbox"/> Large Entity <input type="checkbox"/> Small Entity</p> <p><input type="checkbox"/> A petition for extension of time is also enclosed.</p> <p>The fee for the extension of time is _____.</p> <p><input type="checkbox"/> A check in the amount of _____ is enclosed.</p> <p><input checked="" type="checkbox"/> Charge the amount of the fee to Deposit Account No. <u>18-1945</u>. This sheet is submitted in duplicate.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input checked="" type="checkbox"/> The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. <u>18-1945</u>. This sheet is submitted in duplicate.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"><div> _____ Edward A. Gordon Attorney Reg. No. : 54,130 ROPES & GRAY LLP One International Place Boston, 02110-2624 (617) 951-7066</div><div>Dated: <u>December 17, 2004</u></div></div>			
<p>I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 543609163 US, in an envelope addressed to: MS Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.</p> <div style="display: flex; justify-content: space-between;"><div>Dated: <u>12/17/04</u></div><div>Signature:  (Dawn Marie Class)</div></div>			



COPY

PTO/SB/17 (12-04)

Approved for use through 7/31/2006. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no person are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL For FY 2005		Complete if Known	
		Application Number	09/658207
		Filing Date	September 8, 2000
		First Named Inventor	Robert J. Donaghey
		Examiner Name	L. H. Luu
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27	Art Unit	2141	
TOTAL AMOUNT OF PAYMENT	(\$) 500.00	Attorney Docket No.	BBNT-P01-109

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 18-1945 Deposit Account Name: Ropes & Gray LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or any underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee (\$)	Small Entity Fee (\$)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

<u>Total Claims</u>	<u>Extra Claims</u>	<u>Fee (\$)</u>	<u>Fee Paid (\$)</u>	<u>Multiple Dependent Claims</u>
_____	_____	x _____	= _____	<u>Fee (\$)</u> <u>Fee Paid (\$)</u>
<u>Indep. Claims</u>	<u>Extra Claims</u>	<u>Fee (\$)</u>	<u>Fee Paid (\$)</u>	
_____	_____	x _____	= _____	

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

<u>Total Sheets</u>	<u>Extra Sheets</u>	<u>Number of each additional 50 or fraction thereof</u>	<u>Fee (\$)</u>	<u>Fee Paid (\$)</u>
_____	_____	/50 _____	(round up to a whole number) x _____	= _____

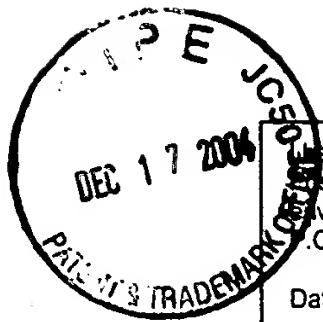
4. OTHER FEE(S)

Non-English Specification, \$130 fee (no small entity discount)	
Other: 1402 Filing a brief in support of an appeal	500.00

SUBMITTED BY			
Signature		Registration No. (Attorney/Agent)	54,130
Name (Print/Type)	Edward A. Gordon	Telephone	(617) 951-7066
		Date	December 17, 2004

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 543609163 US, in an envelope addressed to: MS Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: 12/17/04 Signature: (Dawn Class)



I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 543609163 US, in an envelope addressed to: MS Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: 12/17/04

Signature:

Dawn Class
(Dawn Class)

Docket No.: BBNT-P01-109
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Donaghey et al.

Application No.: 09/658207

Confirmation No.: 3500

Filed: September 8, 2000

Art Unit: 2141

For: SYSTEM AND METHOD FOR SELECTING
AND DISSEMINATING POLICIES

Examiner: L. H. Luu

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

COPY

Dear Sir:

This Appeal Brief is submitted in response to the final Office Action, dated April 20, 2004, and in support of the Notice of Appeal, filed October 18, 2004.

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is BBNT Solutions LLC.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

Appellants are unaware of any related appeals, interferences or judicial proceedings.

III. STATUS OF CLAIMS

Claims 1-25 are pending in this application.

Claims 1-3, 5-7, 9, 10, 13, 14, 16, and 21 have been rejected under 35 U.S.C. § 102(e) as anticipated by Waclawsky (U.S. Patent No. 6,539,026).

Claims 4, 8, 11, 12, 15, 17-20, and 22-25 have been rejected under 35 U.S.C. § 103(a) as unpatentable over Waclawsky in view of McCloghrie et al. (U.S. Patent No. 6,286,052).

Claims 1-3, 5-7, 9, 10, 13, 14, 16, and 21 have been rejected under 35 U.S.C. § 102(e) as anticipated by Waclawsky (U.S. Patent No. 6,539,026).

Claims 4, 8, 11, 12, 15, 17-20, and 22-25 have been rejected under 35 U.S.C. § 103(a) as unpatentable over Waclawsky in view of McCloghrie et al. (U.S. Patent No. 6,286,052).

Claims 1-25 are the subject of the present appeal. These claims are reproduced in the Claim Appendix of this Appeal Brief.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final Office Action, dated April 20, 2004.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In the paragraphs that follow, each of the independent claims that is involved in this appeal will be recited followed in parenthesis by examples of where support can be found in the specification and drawings.

Claim 1 recites a method that ensures policy coherence among a group of peer devices (110), comprising: detecting an addition of a new policy version (650, Fig. 6B; page 15, lines 18-20); generating a message containing the newly added policy version in response to detecting the addition of the new policy version (655, 665, Fig. 6B; page 15, line 20, to page 16, line 7); and transferring the message to the peer devices (670, Fig. 6B; page 16, lines 7-8).

Claim 5 recites a system that ensures policy coherence among a group of peer devices, comprising: means for detecting an addition of one or more new policy versions (120, Fig. 1; 650, Fig. 6B; page 15, lines 18-20); means for generating a message containing the newly added one or more policy versions in response to detecting the addition of one or more policy versions

(120, Fig. 1; 655, 665, Fig. 6B; page 15, line 20, to page 16, line 7); and means for transferring the message to the peer devices (120, Fig. 1; 670, Fig. 6B; page 16, lines 7-8).

Claim 6 recites a computer-readable medium (206, Fig. 2) containing instructions for controlling at least one processor (204, Fig. 2) to perform a method that ensures policy coherence among a group of peer devices, the method comprising: determining whether a policy has been added (650, Fig. 6B; page 15, lines 18-20); generating, in response to a policy being added, a message containing the added policy (655, 665, Fig. 6B; page 15, line 20, to page 16, line 7); and sending the message to the peer devices (670, Fig. 6B; page 16, lines 7-8).

Claim 9 recites a policy server (120, Fig. 1) comprising: a memory configured to store instructions (206, Fig. 2; page 8, lines 16-20); and a processor (204, Fig. 2) configured to execute the instructions to determine whether one or more policy versions have been added (650, Fig. 6B; page 15, lines 18-20), generate, in response to a policy version being added, a message containing the added policy version (655, 665, Fig. 6B; page 15, line 20, to page 16, line 7), and transfer the message to a group of peer devices (670, Fig. 6B; page 16, lines 7-8).

Claim 13 recites a method for distributing policies in a network having at least one anonymous policy server (120, Fig. 1) and at least one anonymous peer device (110, Fig. 1), comprising: requesting a policy from the anonymous policy server (505, 510, Fig. 5; page 13, lines 1-11); determining, via the anonymous policy server, whether an active version of the policy exists (605-615, Fig. 6A; page 14, lines 5-16); and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device (630, 635, Fig. 6A; page 14, line 19, to page 15, line 6).

Claim 17 recites a network comprising: at least one anonymous peer device (110, Fig. 1) configured to: request a policy from at least one anonymous policy server (505, 510, Fig. 5; page 13, lines 1-11), determine whether a received policy is of a desired policy class (515-525, Fig. 5;

page 13, lines 12-18), and implement the received policy when the received policy is an active policy of the desired policy class (540, Fig. 5; page 13, line 20, to page 14, line 3); and at least one anonymous policy server (120, Fig. 1) configured to: receive the request from the at least one anonymous peer device (610, Fig. 6A; page 14, lines 5-9), determine whether any version of the policy requested exists (615, Fig. 6A; page 14, lines 9-16), and transfer all versions of the policy to the peer device, indicating the active version, if any version is determined to exist (620, 630, 635, Fig. 6A; page 14, line 19, to page 15, line 6).

Claim 21 recites a computer-readable medium (206, Fig. 2) containing instructions for controlling at least one processor (204, Fig. 2) to perform a method that distributes policies in a network having a policy server and a peer device, the method comprising: receiving one or more requests, each request indicating a policy of interest to the peer device (610, Fig. 6A; page 14, lines 5-9); determining whether an active version of each of the policies exists (615, Fig. 6A; page 14, lines 9-16); and transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device (620, 630, 635, Fig. 6A; page 14, lines 19-22).

Claim 22 recites a computer-readable medium having a database structure (300, Fig. 3A) comprising: a policy identification field that stores an identifier of a policy (310, Fig. 3A; page 9, lines 17-19); a version field that stores an identifier of a policy version (320, Fig. 3A; page 10, lines 1-2); and a policy content field that stores a content of a policy (350, Fig. 3A; page 10, lines 8-9).

Claim 23 recites a computer-readable medium having a database structure (301, Fig. 3B) comprising: a policy identification field that stores an identifier of a policy (360, Fig. 3B; page 10, lines 14-15); and a version field that stores an identifier of an active policy version (370, Fig. 3B; page 10, lines 15-17).

Claim 24 recites a method for implementing policies, comprising: receiving a message, the message containing an identifier and one or more versions of a policy (520, Fig. 5; page 13, lines 14-16); determining whether the identifier is in a list of policy identifiers (525, Fig. 5; page 13, lines 14-18); discarding the message when the identifier is absent from the list (530, Fig. 5; page 13, lines 19-20); and implementing an active version of the one or more policies when the identifier is present in the list (540, Fig. 5; page 13, line 20, to page 14, line 2).

Claim 25 recites a system for implementing policies comprising: a memory (430, Fig. 4) configured to store instructions and an active policy database, the active policy database containing a list of policy identifiers (page 12, lines 1-10); and a processor (420, Fig. 4) configured to execute the instructions to receive a message, the message containing an identifier and one or more versions of a policy (520, Fig. 5; page 13, lines 14-16), compare the identifier to the list of policy identifiers (525, Fig. 5; page 13, lines 16-18), discard the message when the identifier does not match a policy identifier in the list (530, Fig. 5; page 13, lines 19-20), and implement an active version of the policy when the identifier matches a policy identifier in the list (540, Fig. 5; page 14, lines 1-2).

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-3, 5-7, 9, 10, 13, 14, 16, and 21 stand rejected under 35 U.S.C. § 102(e) as anticipated by Waclawsky (U.S. Patent No. 6,539,026).

B. Claims 4, 8, 11, 12, 15, 17-20, and 22-25 have been rejected under 35 U.S.C. § 103(a) as unpatentable over Waclawsky (U.S. Patent No. 6,539,026) in view of McCloghrie et al. (U.S. Patent No. 6,286,052).

VII. ARGUMENT

A. Rejection under 35 U.S.C. § 102(e) based on Waclawsky (U.S. Patent No. 6,539,026).

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). A proper rejection under 35 U.S.C. § 102 requires that a single reference teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 2 USPQ2d 1051 (Fed. Cir. 1987).

1. Claims 1, 2, 5, 6, and 9.

With the above principles in mind, Appellants' claim 1 is directed to a method that ensures policy coherence among a group of peer devices. The method includes detecting an addition of a new policy version, generating a message containing the newly added policy version in response to detecting the addition of the new policy version, and transferring the message to the peer devices. Waclawsky does not disclose or suggest this combination of features.

For example, Waclawsky does not disclose or suggest generating a message containing the newly added policy version in response to detecting the addition of the new policy version. The Examiner relies on col. 19, line 58, to col. 20, line 29, of Waclawsky for allegedly disclosing this feature (final Office Action, pg. 2). Appellants submit that this section of Waclawsky does not disclose or suggest the above feature of claim 1.

At col. 19, line 58, to col. 20, line 29, Waclawsky discloses:

Step 301 provides the ability to add or remove storage locations 259 from the series of storage locations 259-0 through 259-N each time the step is performed. As such, the invention allows the delay manager 201 to reconfigure itself if changes appear in the network policy 207. That is, the invention allows changes to be made at any time in the network policy 207, such as the addition or removal

of delay categories and/or data attributes. In response, a delay manager configured with the invention can periodically re-execute steps 300 through 302, as illustrated by the periodic re-execution line 310. Alternatively, re-execution of steps 301 through 303 can be triggered by the arrival or manual loading of new network policy information 207 into the data communications device 200. In this manner, the policy controller 250 in the delay manager(s) 201 in the data communications device(s) on network 100 periodically obtain the latest version of the network policy 207 from the network policy server 150 and can reconfigure the delay scheduler 251 and delay controller 252 via control commands 208 as previously described. This allows each data communications device 200 in an entire network to adapt to changes in a distributed network policy 207 with respect to the delay of data 205. Thus if new data types or data having new attributes becomes present on a network, the data communications devices 200 that use this invention can adapt to the new delay requirements without manually updating hardware or software within the devices 200.

This aspect of the invention thus ensures that a networked data communications device 200 is able to update itself with the latest network policy 207. Prior art network policy updates are typically performed by sending the network policy to each device by an affirmative act on the part of the network policy server 150. This invention eliminates the need to do this and places the burden for obtaining network policy updates on the data communication devices 200 themselves. As such, if there are hundreds or thousands of data communications devices 200 in the network, the load caused by network policy updates is distributed across each device.

This section of Waclawsky specifically discloses that policy controllers 250 in network devices 200 periodically obtain the latest version of network policy 207 from network policy server 150 (col. 20, lines 4-10). Waclawsky does not disclose or suggest, however, that policy controllers 250 obtain the latest version of network policy in response to detecting the addition of a new policy version, as required by claim 1. By stark contrast, Waclawsky specifically discloses that the obtaining of the latest version of network policy 207 occurs periodically. Moreover, this section of Waclawsky does not disclose or suggest that network policy server 150 (or any other device) generates a message containing a newly added policy version in response to detecting the addition of the new policy version, as required by claim 1. The Examiner has not logically explained how Waclawsky's disclosure that policy controllers 250 periodically obtain the latest version of network policy can reasonably be said to correspond to generating a message

containing the newly added policy version in response to detecting the addition of the new policy version, as required by claim 1. The Examiner has not pointed to any section of Waclawsky that discloses or suggests generating a message containing the newly added policy version in response to detecting the addition of the new policy version, as required by claim 1.

Since Waclawsky does not disclose generating a message containing the newly added policy version in response to detecting the addition of the new policy version, Waclawsky cannot disclose transferring the message to the peer devices, as also required by claim 1.

For at least the foregoing reasons, Appellants submit that the rejection of claim 1 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

2. Claims 3, 7, and 10.

Claim 3 recites determining whether a policy version has become newly active, generating a second message containing an indication of the newly active policy version, and sending the second message to the peer devices. Waclawsky does not disclose or suggest this combination of features.

At the outset, Appellants' note that claim 3 depends from claim 1 and, therefore, is not anticipated by Waclawsky for at least the reasons given above with respect to claim 1. Moreover, this claim is not anticipated by Waclawsky for reasons of its own.

The Examiner relies on col. 19, line 58, to col. 20, line 29, of Waclawsky for allegedly disclosing the features of claim 3 (final Office Action, pg. 3). Appellants disagree.

At col. 19, line 58, to col. 20, line 29, Waclawsky discloses:

Step 301 provides the ability to add or remove storage locations 259 from the series of storage locations 259-0 through 259-N each time the step is performed. As such, the invention allows the delay manager 201 to reconfigure itself if changes appear in the network policy 207. That is, the invention allows changes to be made at any time in the network policy 207, such as the addition or removal

of delay categories and/or data attributes. In response, a delay manager configured with the invention can periodically re-execute steps 300 through 302, as illustrated by the periodic re-execution line 310. Alternatively, re-execution of steps 301 through 303 can be triggered by the arrival or manual loading of new network policy information 207 into the data communications device 200. In this manner, the policy controller 250 in the delay manager(s) 201 in the data communications device(s) on network 100 periodically obtain the latest version of the network policy 207 from the network policy server 150 and can reconfigure the delay scheduler 251 and delay controller 252 via control commands 208 as previously described. This allows each data communications device 200 in an entire network to adapt to changes in a distributed network policy 207 with respect to the delay of data 205. Thus if new data types or data having new attributes becomes present on a network, the data communications devices 200 that use this invention can adapt to the new delay requirements without manually updating hardware or software within the devices 200.

This aspect of the invention thus ensures that a networked data communications device 200 is able to update itself with the latest network policy 207. Prior art network policy updates are typically performed by sending the network policy to each device by an affirmative act on the part of the network policy server 150. This invention eliminates the need to do this and places the burden for obtaining network policy updates on the data communication devices 200 themselves. As such, if there are hundreds or thousands of data communications devices 200 in the network, the load caused by network policy updates is distributed across each device.

This section of Waclawsky discloses the ability to reconfigure delay manager 201 of a network device 200 based on a network policy. This section of Waclawsky in no way discloses or suggests, however, determining whether a policy version has become active, generating a second message containing an indication of the newly active policy version, and sending the second message to the peer devices, as required by claim 3. The Examiner has not logically explained how the above section of Waclawsky can reasonably be construed to disclose the above features of claim 3.

The Examiner further alleges that "Waclawsky teaches the data communication device periodically determines whether another latest version (at time t1 which is later than time t) of network policy in the network policy server has become newly active. The network policy server generates another message that contains the another latest version of the network policy;

and sending the another message to the data communication device" and points to col. 19, line 58, to col. 20, line 29, of Waclawsky for support (final Office Action, pg. 5). Appellants submit that the Examiner has mischaracterized the disclosure of Waclawsky.

Contrary to the Examiner's allegation, Waclawsky does not disclose or suggest that the data communication device periodically determines whether another latest version of a network policy has become newly active. Instead, Waclawsky discloses that the data communication devices periodically obtain the latest version of network policy 207 (col. 20, lines 4-10).

Contrary to the Examiner's allegation, Waclawsky does not disclose or suggest that the data communication devices periodically obtaining the latest version of network policy 207 involves determining whether a policy version has become newly active, generating a second message containing an indication of the newly active policy version, or sending the second message to peer devices, as required by claim 3. The Examiner has not logically explained how the above section of Waclawsky can reasonably be construed to disclose the features of claim 3.

For at least the foregoing reasons, Appellants submit that the rejection of claim 3 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

3. Claim 13.

Independent claim 13 is directed to a method for distributing policies in a network having at least one anonymous policy server and at least one anonymous peer device. The method includes requesting a policy from the anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device. Waclawsky does not disclose or suggest this combination of features.

For example, Waclawsky does not disclose or suggest requesting a policy from an anonymous policy server. Waclawsky does not disclose or suggest that policy server 150 is an anonymous policy server, as required by claim 13. With respect to this feature, the Examiner alleges that "Waclawsky did not discuss device authentication prior to obtain the updates. Therefore, the network policy server and the devices are anonymous" (final Office Action, pg. 5). Appellants disagree.

The mere fact that Waclawsky does not disclose device authentication in no way discloses or suggests that network policy server 150 and network devices 200 are anonymous. In fact, Waclawsky specifically discloses that network devices 200 are access servers, routers, switches, hubs, bridges, gateways, proxy servers, concentrators, repeaters, and similar data transfer devices (col. 7, lines 2-6). Such network devices are typically not anonymous since anonymity of these devices could hinder the transfer of data through communications network 100. For example, routers typically know the identity of other routers in proximity to themselves so as to know how to route data through a network. The Examiner has not pointed to any section of Waclawsky that supports the allegation that network policy server 150 and network devices 200 are anonymous.

Since Waclawsky does not disclose or suggest that network policy server 150 and network devices 200 are anonymous, Waclawsky cannot disclose or suggest requesting a policy from an anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to an anonymous peer device, as required by claim 13.

Even assuming, for the sake of argument, that one skilled in the art could reasonably construe Waclawsky's network policy server 150 and network devices 200 as anonymous,

Appellants submit that Waclawsky does not disclose or suggest requesting a policy from an anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to an anonymous peer device, as required by claim 13. The Examiner did not address the combination of features recited in Appellants' claim 13 (see pp. 2-3 of final Office Action). Instead, the Examiner merely addressed the features of Appellants' claims 1-3. Appellants' claim 13 recites features not recited in claims 1-3. Therefore, a *prima facie* case of anticipation has not been established with respect to claim 13.

Nonetheless, Waclawsky discloses that a data communications device 200 can request policy updates from network server 150 when needed (col. 20, lines 18-29). Waclawsky in no way discloses or suggests, however, requesting a policy from an anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to an anonymous peer device, as required by claim 13.

For at least the foregoing reasons, Appellants submit that the rejection of claim 13 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

4. Claim 14.

Claim 14 recites that requesting a policy from the anonymous policy server includes generating, via the anonymous peer device, a policy request, where the policy request contains a policy identifier; and transferring the policy request to the anonymous policy server. Waclawsky does not disclose or suggest this combination of features.

At the outset, Appellants' note that claim 14 depends from claim 13 and, therefore, is not anticipated by Waclawsky for at least the reasons given above with respect to claim 13.

Moreover, this claim is not anticipated by Waclawsky for reasons of its own.

For example, Waclawsky does not disclose or suggest generating, via the anonymous peer device, a policy request, where the policy request contains a policy identifier. The Examiner has not addressed this feature in the final Office Action. Therefore, a *prima facie* case of anticipation has not been established with respect to claim 14.

Nonetheless, as set forth above, Waclawsky discloses that a data communications device 200 can request policy updates from network server 150 when needed (col. 20, lines 18-29). Waclawsky does not disclose or suggest, however, that data communications device 200 is an anonymous peer device or that data communications device 200 generates a policy request that includes a policy identifier, as required by claim 14.

For at least the foregoing reasons, Appellants submit that the rejection of claim 14 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

5. Claim 16.

Claim 16 recites receiving, via the anonymous peer device, a policy; determining whether the received policy is the requested policy; discarding the received policy when the received policy is not the requested policy; and implementing the received policy when the received policy is the requested policy. Waclawsky does not disclose or suggest this combination of features.

At the outset, Appellants' note that claim 16 depends from claim 13 and, therefore, is not anticipated by Waclawsky for at least the reasons given above with respect to claim 13. Moreover, this claim is not anticipated by Waclawsky for reasons of its own.

For example, Waclawsky does not disclose or suggest determining whether a received policy is the requested policy or discarding the received policy when the received policy is not the requested policy. The Examiner has not addressed this feature in the final Office Action. Therefore, a *prima facie* case of anticipation has not been established with respect to claim 16.

Nonetheless, as set forth above, Waclawsky discloses that a data communications device 200 can request policy updates from network server 150 when needed (col. 20, lines 18-29). Waclawsky does not disclose or suggest, however, that data communications device 200 is an anonymous peer device or that data communications device 200 determines whether a received policy is the requested policy or discards the received policy when the received policy is not the requested policy, as required by claim 16.

For at least the foregoing reasons, Appellants submit that the rejection of claim 16 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

6. Claim 21.

Independent claim 21 is directed to a computer-readable medium containing instructions for controlling at least one processor to perform a method that distributes policies in a network having a policy server and a peer device. The method includes receiving one or more requests, where each request indicates a policy of interest to the peer device; determining whether an active version of each of the policies exists; and transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device recites receiving, via the anonymous peer device, a policy. Waclawsky does not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the combination of features recited in Appellants' claim 21. Therefore, the Examiner has not established a *prima facie* case of anticipation with respect to claim 21.

Nonetheless, Waclawsky does not disclose or suggest determining whether an active version of each of the policies exists and transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device. To the contrary, Waclawsky discloses that policy controller 250 in network devices 200 periodically obtains the latest version of network policy 207 from network policy server 150 (col. 20, lines 4-10).

Since Waclawsky does not disclose or suggest all of the features of claim 21, Waclawsky does not anticipate claim 21.

For at least the foregoing reasons, Appellants submit that the rejection of claim 21 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

B. Rejection under 35 U.S.C. § 103(a) based on Waclawsky (U.S. Patent No. 6,539,026) and McCloghrie et al. (U.S. Patent No. 6,286,052).

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the Examiner must provide a factual basis to support the conclusion of obviousness. In re Warner, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967). Based upon the objective evidence of record, the Examiner is required to make the factual inquiries mandated by Graham v. John Deere Co., 86 S.Ct. 684, 383 U.S. 1, 148 USPQ 459 (1966). The Examiner is also required to explain how and why one having ordinary

skill in the art would have been realistically motivated to modify an applied reference and/or combine applied references to arrive at the claimed invention. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988).

In establishing the requisite motivation, it has been consistently held that the requisite motivation to support the conclusion of obviousness is not an abstract concept, but must stem from the prior art as a whole to impel one having ordinary skill in the art to modify a reference or to combine references with a reasonable expectation of successfully achieving some particular realistic objective. See, for example, Interconnect Planning Corp. v. Feil, 227 USPQ 543 (Fed. Cir. 1985). Consistent legal precedent admonishes against the indiscriminate combination of prior art references. Carella v. Starlight Archery, 804 F.2d 135, 231 USPQ 644 (Fed. Cir. 1986); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985).

1. Claims 4, 8, 11, and 12.

With the above principles in mind, Appellants' claim 4 depends indirectly from claim 1. The disclosure of McCloghrie et al. does not remedy the deficiencies in the disclosure of Waclawsky set forth above with respect to claim 1. Therefore, claim 4 is patentable over Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1. Moreover, this claim is patentable over Waclawsky and McCloghrie et al. for reasons of its own.

Claim 4 recites storing, in response to a policy version becoming newly active, an identifier of the newly active policy in an active policy database, where the active policy database stores a list of active policy identifiers. The Examiner admits that Waclawsky does not disclose these features and relies on col. 14, lines 25-44, of McCloghrie et al. for allegedly

disclosing the features of claim 4 (final Office Action, pp. 4-6). Appellants submit that McCloghrie et al. does not disclose the features of claim 4.

At col. 14, lines 25-44, McCloghrie et al. discloses:

The first policy binding 552a, for example, may contain an encoded copy of the source port identified by program 224 with the SetSourcePort() call 414a and stored at the respective traffic flow data structure 234. More specifically, message generator 230 loads policy identifier field 562a with the type or instance of the policy element (e.g., "source port"). In the preferred embodiment, this name is a Policy Identifier (PID) as specified in the Internet Engineering Task Force (IETF) draft document COPS Usage for Differentiated Services submitted by the Network Working Group, dated December 1998, and incorporated herein by reference in its entirety. A PID specifies a particular policy class (e.g., a type of policy data item) or policy instance (e.g., a particular instance of a given policy class) in a hierarchical arrangement. The Policy ID type field 560a contains a predefined value reflecting that field 562a contains information in PID format. Component 226 preferably includes a Policy Information Base (PIB) for use in deriving the particular policy identifiers, as described in COPS Usage for Differentiated Services.

This section of McCloghrie et al. discloses placing a Policy Identifier (PID) in a message. This section of McCloghrie et al. does not disclose or suggest, however, storing a PID of a newly active policy in an active policy database, in response to a policy version becoming newly active, where the active policy database stores a list of active policy identifiers, as required by claim 4.

Even assuming, for the sake of argument, that one skilled in the art could reasonably construe the disclosure of McCloghrie et al. to disclose the features of claim 4, Appellants submit that one skilled in the art would not have been motivated to combine the teachings of Waclawsky and McCloghrie et al. in the manner suggested by the Examiner, absent impermissible hindsight. With respect to motivation, the Examiner alleges that "[i]t would have been obvious ... to combine the teachings of Waclawsky and McCloghrie to stores a list of active policy identifiers in an active policy database because it would allow a device to be

configured for a particular services using active policies stored in the active policy database" (final Office Action, pp. 4 and 6). Appellants disagree.

The Examiner has not pointed to any section of Waclawsky or McCloghrie et al. to support the Examiner's motivation to combine McCloghrie et al. with Waclawsky. Waclawsky does not disclose or suggest an active policy database. The Examiner's motivation falls short of logically explaining why one would seek to incorporate an active policy database into the Waclawsky system. The Examiner's motivation is merely conclusory and insufficient for establishing a *prima facie* case of obviousness.

For at least the foregoing reasons, Appellants submit that the rejection of claim 4 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

2. Claims 15 and 20.

Claim 15 depends indirectly from claim 13. The disclosure of McCloghrie et al. does not remedy the deficiencies in the disclosure of Waclawsky set forth above with respect to claim 13. Therefore, claim 15 is patentable over Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 13. Moreover, this claim is patentable over Waclawsky and McCloghrie et al. for reasons of its own.

Claim 15 recites that the determining, via the anonymous policy server, whether an active version of the policy exists includes comparing the identifier in the policy request to a list of active policy identifiers. Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, do not disclose or suggest this feature.

The Examiner has not addressed the feature recited in claim 15. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation,

Appellants' claims 1-4 do not recite comparing the identifier in the policy request to a list of active policy identifiers, as required by claim 15. Since the Examiner has not addressed the feature of claim 15, a *prima facie* case of obviousness has not been established with respect to claim 15.

For at least the foregoing reasons, Appellants submit that the rejection of claim 15 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

3. Claims 17-19.

Claim 17 is directed to network that includes at least one anonymous peer device and at least one anonymous policy server. The at least one anonymous peer device is configured to request a policy from at least one anonymous policy server, determine whether a received policy is of a desired policy class, and implement the received policy when the received policy is an active policy of the desired policy class. The at least one anonymous policy server is configured to receive the request from the at least one anonymous peer device, determine whether any version of the policy requested exists, and transfer all versions of the policy to the peer device, indicating the active version, if any version is determined to exist. Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, Waclawsky and McCloghrie et al. do not disclose or suggest at least one anonymous peer device and at least one anonymous policy server. As set forth above, Waclawsky does not disclose or suggest that policy server 150 is an anonymous policy server. Moreover, Waclawsky does not disclose or suggest that network devices 200 are anonymous peer devices. McCloghrie et al. discloses a policy server 216, but does not disclose or suggest

that policy server 216 is an anonymous policy server. Moreover, McCloghrie et al. does not disclose or suggest at least one anonymous peer device.

As discussed above, the Examiner alleges that "Waclawsky did not discuss device authentication prior to obtain the updates. Therefore, the network policy server and the devices are anonymous" (final Office Action, pg. 5). Appellants disagree.

The mere fact that Waclawsky does not disclose device authentication in no way discloses or suggests that network policy server 150 and network devices 200 are anonymous. In fact, Waclawsky specifically discloses that network devices 200 are access servers, routers, switches, hubs, bridges, gateways, proxy servers, concentrators, repeaters, and similar data transfer devices (col. 7, lines 2-6). Such network devices are typically not anonymous since anonymity of these devices could hinder the transfer of data through communications network 100. For example, routers typically know the identity of other routers in proximity to themselves so as to know how to route data through a network. The Examiner has not pointed to any section of Waclawsky that supports the allegation that network policy server 150 and network devices 200 are anonymous.

Even assuming, for the sake of argument, that Waclawsky's network policy server 150 and network devices 200 could be considered anonymous, Waclawsky and McCloghrie et al. do not disclose features of Appellants' claim 17. For example, Waclawsky and McCloghrie et al. do not disclose or suggest at least one anonymous peer device that is configured to determine whether a received policy is of a desired policy class and implement the received policy when the received policy is an active policy of the desired policy class or at least one anonymous policy server that is configured to determine whether any version of a requested policy exists and transfer all versions of the policy to the peer device, indicating the active version if any version is determined to exist, as required by claim 17.

The Examiner has not addressed the features of claim 17. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above features of claim 17. Since the Examiner has not addressed the above features of claim 17, a *prima facie* case of obviousness has not been established with respect to claim 17.

For at least the foregoing reasons, Appellants submit that the rejection of claim 17 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

4. Claim 22.

Independent claim 22 recites a computer-readable medium having a database structure that includes a policy identification field that stores an identifier of a policy, a version field that stores an identifier of a policy version, and a policy content field that stores a content of a policy. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 22. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above features of claim 22. Since the Examiner has not addressed the above features of claim 22, a *prima facie* case of obviousness has not been established with respect to claim 22.

For at least the foregoing reasons, Appellants submit that the rejection of claim 22 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

5. Claim 23.

Independent claim 23 recites a computer-readable medium having a database structure that includes a policy identification field that stores an identifier of a policy, and a version field that stores an identifier of an active policy version. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 23. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above features of claim 23. Since the Examiner has not addressed the above features of claim 23, a *prima facie* case of obviousness has not been established with respect to claim 23.

For at least the foregoing reasons, Appellants submit that the rejection of claim 23 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

6. Claim 24.

Independent claim 24 is directed to a method for implementing policies. The method includes receiving a message, where the message contains an identifier and one or more versions of a policy; determining whether the identifier is in a list of policy identifiers; discarding the message when the identifier is absent from the list; and implementing an active version of the one or more policies when the identifier is present in the list. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 24. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above

combination of features of claim 24. Since the Examiner has not addressed the above features of claim 24, a *prima facie* case of obviousness has not been established with respect to claim 24.

For at least the foregoing reasons, Appellants submit that the rejection of claim 24 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

7. Claim 25.

Independent claim 25 is directed to a system for implementing policies. The system includes a memory and a processor. The memory is configured to store instructions and an active policy database, where the active policy database contains a list of policy identifiers. The processor is configured to execute the instructions to receive a message, where the message contains an identifier and one or more versions of a policy, compare the identifier to the list of policy identifiers, discard the message when the identifier does not match a policy identifier in the list, and implement an active version of the policy when the identifier matches a policy identifier in the list. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 25. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above combination of features of claim 25. Since the Examiner has not addressed the above features of claim 25, a *prima facie* case of obviousness has not been established with respect to claim 25.

For at least the foregoing reasons, Appellants submit that the rejection of claim 25 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

Application No.: 09/658207

Docket No.: BBNT-P01-109


VIII. CONCLUSION

In view of the foregoing arguments, Appellants respectfully solicit the Honorable Board to reverse the Examiner's rejections of claims 1-25 under 35 U.S.C. §§ 102 and 103.

Applicant believes no fee is due with this response other than as reflected on the enclosed fee transmittal. However, if a fee is due, please charge our Deposit Account No. 18-1945, under Order No. BBNT-P01-109 from which the undersigned is authorized to draw.

Dated: December 17, 2004

Respectfully submitted,

By 

Edward A. Gordon

Registration No.: 54,130

ROPES & GRAY LLP

One International Place

Boston, 02110-2624

(617) 951-7000

(617) 951-7050 (Fax)

Attorneys/Agents For Applicant

CLAIM APPENDIX

1. A method that ensures policy coherence among a group of peer devices, comprising:
 - detecting an addition of a new policy version;
 - generating a message containing the newly added policy version in response to detecting the addition of the new policy version; and
 - transferring the message to the peer devices.
2. The method of claim 1 wherein the newly added policy version is a policy that relates to at least one of system administration, system security, command and control, and courses of action.
3. The method of claim 1 further comprising:
 - determining whether a policy version has become newly active;
 - generating a second message containing an indication of the newly active policy version; and
 - sending the second message to the peer devices.
4. The method of claim 3 further comprising:
 - storing, in response to a policy version becoming newly active, an identifier of the newly active policy in an active policy database, the active policy database storing a list of active policy identifiers.

5. A system that ensures policy coherence among a group of peer devices, comprising:
- means for detecting an addition of one or more new policy versions;
 - means for generating a message containing the newly added one or more policy versions in response to detecting the addition of one or more policy versions; and
 - means for transferring the message to the peer devices.
6. A computer-readable medium containing instructions for controlling at least one processor to perform a method that ensures policy coherence among a group of peer devices, the method comprising:
- determining whether a policy has been added;
 - generating, in response to a policy being added, a message containing the added policy; and
 - sending the message to the peer devices.
7. The computer-readable medium of claim 6 wherein the method further comprises:
- determining whether a version of one of a group of policies has become active;
 - generating a second message containing the active version;
 - transferring the second message to the peer devices.
8. The computer-readable medium of claim 7 wherein the method further comprises:
- storing an identifier of the newly active policy in an active policy database, the active policy database including a list of active policy identifiers.

9. A policy server comprising:
 - a memory configured to store instructions; and
 - a processor configured to execute the instructions to determine whether one or more policy versions have been added, generate, in response to a policy version being added, a message containing the added policy version, and transfer the message to a group of peer devices.
10. The policy server of claim 9 wherein the processor is further configured to:
 - detect a policy version becoming newly active,
 - generate, in response to the detecting, a second message containing the newly active policy version, and
 - transmit the second message to the group of peer devices.
11. The policy server of claim 10 wherein the memory is further configured to:
 - store an active policy database containing a list of identifiers of active policies.
12. The policy server of claim 11 wherein the processor is further configured to:
 - store, in response to a policy becoming active, an identifier of the newly active policy in the active policy database.
13. A method for distributing policies in a network having at least one anonymous policy server and at least one anonymous peer device, comprising:
 - requesting a policy from the anonymous policy server;

determining, via the anonymous policy server, whether an active version of the policy exists; and

transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device.

14. The method of claim 13 wherein the requesting includes:

generating, via the anonymous peer device, a policy request, the policy request containing a policy identifier; and

transferring the policy request to the anonymous policy server.

15. The method of claim 14 wherein the determining includes:

comparing the identifier in the policy request to a list of active policy identifiers.

16. The method of claim 13 further comprising:

receiving, via the anonymous peer device, a policy;

determining whether the received policy is the requested policy;

discarding the received policy when the received policy is not the requested policy; and

implementing the received policy when the received policy is the requested policy.

17. A network comprising:

at least one anonymous peer device configured to:

request a policy from at least one anonymous policy server,

determine whether a received policy is of a desired policy class, and
implement the received policy when the received policy is an active
policy of the desired policy class; and

at least one anonymous policy server configured to:

receive the request from the at least one anonymous peer device,
determine whether any version of the policy requested exists, and
transfer all versions of the policy to the peer device, indicating the active
version, if any version is determined to exist.

18. The network of claim 17 wherein the at least one anonymous peer device is
further configured to:

discard the received policy when the received policy is not of the requested policy
class.

19. The network of claim 17 wherein, when requesting, the at least one anonymous
peer device is configured to:

generate a policy request, the policy request containing an identifier that identifies
the requested policy, and
transfer the policy request to the at least one anonymous policy server.

20. The network of claim 18 wherein, when determining, the at least one anonymous
policy server is configured to:

compare the identifier in the policy request to a list of active policy identifiers.

21. A computer-readable medium containing instructions for controlling at least one processor to perform a method that distributes policies in a network having a policy server and a peer device, the method comprising:

receiving one or more requests, each request indicating a policy of interest to the peer device;

determining whether an active version of each of the policies exists; and

transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device.

22. A computer-readable medium having a database structure comprising:

a policy identification field that stores an identifier of a policy;

a version field that stores an identifier of a policy version; and

a policy content field that stores a content of a policy.

23. A computer-readable medium having a database structure comprising:

a policy identification field that stores an identifier of a policy; and

a version field that stores an identifier of an active policy version.

24. A method for implementing policies, comprising:

receiving a message, the message containing an identifier and one or more versions of a policy;

determining whether the identifier is in a list of policy identifiers;

discarding the message when the identifier is absent from the list; and

implementing an active version of the one or more policies when the identifier is present in the list.

25. A system for implementing policies comprising:
 - a memory configured to store instructions and an active policy database, the active policy database containing a list of policy identifiers; and
 - a processor configured to execute the instructions to receive a message, the message containing an identifier and one or more versions of a policy, compare the identifier to the list of policy identifiers, discard the message when the identifier does not match a policy identifier in the list, and implement an active version of the policy when the identifier matches a policy identifier in the list.

Via: Express Mail EV 543609163 US
Inventor: Donaghey et al. Atty Dkt No.: BBNT-P01-109

Application No.: 09/658207 Filing Date: September 8, 2000

Title: SYSTEM AND METHOD FOR SELECTING AND DISSEMINATING POLICIES

Documents Filed:
Appeal Brief Transmittal (1 page)

Fee Transmittal (1 page)

Appeal Brief (32 pages)

Charge \$500.00 to deposit account 18-1945

Return postcard

Sender's Initials: EAG/dmc Date: December 17, 2004

9611640-1



COPY

TRANSMITTAL OF APPEAL BRIEF			Docket No. BBNT-P01-109
In re Application of: Donaghey et al.			
Application No. 09/658207	Filing Date September 8, 2000	Examiner L. H. Luu	Group Art Unit 2141
Invention: SYSTEM AND METHOD FOR SELECTING AND DISSEMINATING POLICIES			

TO THE COMMISSIONER OF PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: October 18, 2004.

The fee for filing this Appeal Brief is \$ 500.00.

☒ Large Entity ☐ Small Entity

☐ A petition for extension of time is also enclosed.

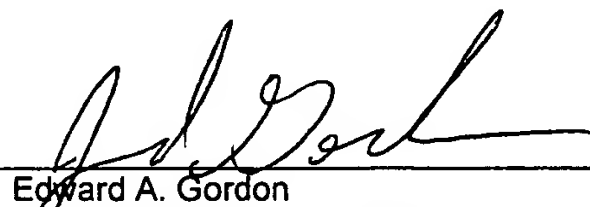
The fee for the extension of time is _____.

☐ A check in the amount of _____ is enclosed.

☒ Charge the amount of the fee to Deposit Account No. 18-1945.
This sheet is submitted in duplicate.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 18-1945.
This sheet is submitted in duplicate.



Edward A. Gordon

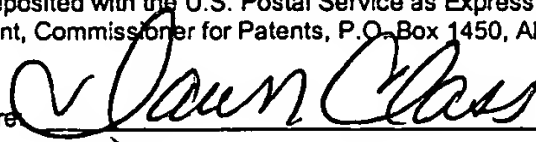
Attorney Reg. No. : 54,130
ROPES & GRAY LLP
One International Place
Boston, 02110-2624
(617) 951-7066

Dated: December 17, 2004

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 543609163 US, in an envelope addressed to: MS Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: 12/17/04

Signature



(Dawn Marie Class)



Effective on 12/08/2004. Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).		Complete if Known	
FEE TRANSMITTAL For FY 2005		Application Number	09/658207
		Filing Date	September 8, 2000
		First Named Inventor	Robert J. Donaghey
		Examiner Name	L. H. Luu
		Art Unit	2141
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27		Attorney Docket No.	BBNT-P01-109
TOTAL AMOUNT OF PAYMENT	(\$) 500.00		

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 18-1945 Deposit Account Name: Ropes & Gray LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or any underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee (\$)	Small Entity Fee (\$)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

Total Claims Extra Claims Fee (\$) Fee Paid (\$)

_____ - = _____ x _____ = _____

Multiple Dependent Claims

Fee (\$) Fee Paid (\$)

_____ _____

Indep. Claims Extra Claims Fee (\$) Fee Paid (\$)

_____ - = _____ x _____ = _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets Extra Sheets Number of each additional 50 or fraction thereof Fee (\$) Fee Paid (\$)

_____ - 100 = _____ / 50 _____ (round up to a whole number) x _____ = _____

4. OTHER FEE(S)

Non-English Specification, \$130 fee (no small entity discount)

Other: 1402 Filing a brief in support of an appeal

Fees Paid (\$)

500.00

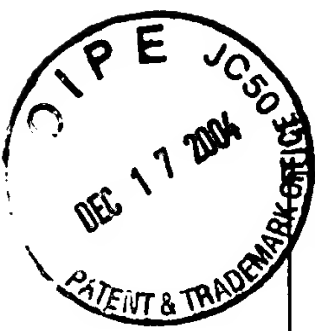
SUBMITTED BY			
Signature		Registration No. (Attorney/Agent)	54,130
Name (Print/Type)	Edward A. Gordon	Telephone	(617) 951-7066
		Date	December 17, 2004

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 543609163 US, in an envelope addressed to: MS Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: 12/17/04

Signature:

(Dawn Class)



I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 543609163 US, in an envelope addressed to: MS Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: 12/17/04 Signature: Dawn Class
(Dawn Class)

Docket No.: BBNT-P01-109
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Donaghey et al.

Application No.: 09/658207

Confirmation No.: 3500

Filed: September 8, 2000

Art Unit: 2141

For: SYSTEM AND METHOD FOR SELECTING
AND DISSEMINATING POLICIES

Examiner: L. H. Luu

12/22/2004 SDIRETA1 00000001 181945 09658207

01 FC:1402

500.00 DA

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in response to the final Office Action, dated April 20, 2004, and in support of the Notice of Appeal, filed October 18, 2004.

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is BBNT Solutions LLC.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

Appellants are unaware of any related appeals, interferences or judicial proceedings.

III. STATUS OF CLAIMS

Claims 1-25 are pending in this application.

Claims 1-3, 5-7, 9, 10, 13, 14, 16, and 21 have been rejected under 35 U.S.C. § 102(e) as anticipated by Waclawsky (U.S. Patent No. 6,539,026).

Claims 4, 8, 11, 12, 15, 17-20, and 22-25 have been rejected under 35 U.S.C. § 103(a) as unpatentable over Waclawsky in view of McCloghrie et al. (U.S. Patent No. 6,286,052).

Claims 1-3, 5-7, 9, 10, 13, 14, 16, and 21 have been rejected under 35 U.S.C. § 102(e) as anticipated by Waclawsky (U.S. Patent No. 6,539,026).

Claims 4, 8, 11, 12, 15, 17-20, and 22-25 have been rejected under 35 U.S.C. § 103(a) as unpatentable over Waclawsky in view of McCloghrie et al. (U.S. Patent No. 6,286,052).

Claims 1-25 are the subject of the present appeal. These claims are reproduced in the Claim Appendix of this Appeal Brief.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final Office Action, dated April 20, 2004.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In the paragraphs that follow, each of the independent claims that is involved in this appeal will be recited followed in parenthesis by examples of where support can be found in the specification and drawings.

Claim 1 recites a method that ensures policy coherence among a group of peer devices (110), comprising: detecting an addition of a new policy version (650, Fig. 6B; page 15, lines 18-20); generating a message containing the newly added policy version in response to detecting the addition of the new policy version (655, 665, Fig. 6B; page 15, line 20, to page 16, line 7); and transferring the message to the peer devices (670, Fig. 6B; page 16, lines 7-8).

Claim 5 recites a system that ensures policy coherence among a group of peer devices, comprising: means for detecting an addition of one or more new policy versions (120, Fig. 1; 650, Fig. 6B; page 15, lines 18-20); means for generating a message containing the newly added one or more policy versions in response to detecting the addition of one or more policy versions

(120, Fig. 1; 655, 665, Fig. 6B; page 15, line 20, to page 16, line 7); and means for transferring the message to the peer devices (120, Fig. 1; 670, Fig. 6B; page 16, lines 7-8).

Claim 6 recites a computer-readable medium (206, Fig. 2) containing instructions for controlling at least one processor (204, Fig. 2) to perform a method that ensures policy coherence among a group of peer devices, the method comprising: determining whether a policy has been added (650, Fig. 6B; page 15, lines 18-20); generating, in response to a policy being added, a message containing the added policy (655, 665, Fig. 6B; page 15, line 20, to page 16, line 7); and sending the message to the peer devices (670, Fig. 6B; page 16, lines 7-8).

Claim 9 recites a policy server (120, Fig. 1) comprising: a memory configured to store instructions (206, Fig. 2; page 8, lines 16-20); and a processor (204, Fig. 2) configured to execute the instructions to determine whether one or more policy versions have been added (650, Fig. 6B; page 15, lines 18-20), generate, in response to a policy version being added, a message containing the added policy version (655, 665, Fig. 6B; page 15, line 20, to page 16, line 7), and transfer the message to a group of peer devices (670, Fig. 6B; page 16, lines 7-8).

Claim 13 recites a method for distributing policies in a network having at least one anonymous policy server (120, Fig. 1) and at least one anonymous peer device (110, Fig. 1), comprising: requesting a policy from the anonymous policy server (505, 510, Fig. 5; page 13, lines 1-11); determining, via the anonymous policy server, whether an active version of the policy exists (605-615, Fig. 6A; page 14, lines 5-16); and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device (630, 635, Fig. 6A; page 14, line 19, to page 15, line 6).

Claim 17 recites a network comprising: at least one anonymous peer device (110, Fig. 1) configured to: request a policy from at least one anonymous policy server (505, 510, Fig. 5; page 13, lines 1-11), determine whether a received policy is of a desired policy class (515-525, Fig. 5;

page 13, lines 12-18), and implement the received policy when the received policy is an active policy of the desired policy class (540, Fig. 5; page 13, line 20, to page 14, line 3); and at least one anonymous policy server (120, Fig. 1) configured to: receive the request from the at least one anonymous peer device (610, Fig. 6A; page 14, lines 5-9), determine whether any version of the policy requested exists (615, Fig. 6A; page 14, lines 9-16), and transfer all versions of the policy to the peer device, indicating the active version, if any version is determined to exist (620, 630, 635, Fig. 6A; page 14, line 19, to page 15, line 6).

Claim 21 recites a computer-readable medium (206, Fig. 2) containing instructions for controlling at least one processor (204, Fig. 2) to perform a method that distributes policies in a network having a policy server and a peer device, the method comprising: receiving one or more requests, each request indicating a policy of interest to the peer device (610, Fig. 6A; page 14, lines 5-9); determining whether an active version of each of the policies exists (615, Fig. 6A; page 14, lines 9-16); and transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device (620, 630, 635, Fig. 6A; page 14, lines 19-22).

Claim 22 recites a computer-readable medium having a database structure (300, Fig. 3A) comprising: a policy identification field that stores an identifier of a policy (310, Fig. 3A; page 9, lines 17-19); a version field that stores an identifier of a policy version (320, Fig. 3A; page 10, lines 1-2); and a policy content field that stores a content of a policy (350, Fig. 3A; page 10, lines 8-9).

Claim 23 recites a computer-readable medium having a database structure (301, Fig. 3B) comprising: a policy identification field that stores an identifier of a policy (360, Fig. 3B; page 10, lines 14-15); and a version field that stores an identifier of an active policy version (370, Fig. 3B; page 10, lines 15-17).

Claim 24 recites a method for implementing policies, comprising: receiving a message, the message containing an identifier and one or more versions of a policy (520, Fig. 5; page 13, lines 14-16); determining whether the identifier is in a list of policy identifiers (525, Fig. 5; page 13, lines 14-18); discarding the message when the identifier is absent from the list (530, Fig. 5; page 13, lines 19-20); and implementing an active version of the one or more policies when the identifier is present in the list (540, Fig. 5; page 13, line 20, to page 14, line 2).

Claim 25 recites a system for implementing policies comprising: a memory (430, Fig. 4) configured to store instructions and an active policy database, the active policy database containing a list of policy identifiers (page 12, lines 1-10); and a processor (420, Fig. 4) configured to execute the instructions to receive a message, the message containing an identifier and one or more versions of a policy (520, Fig. 5; page 13, lines 14-16), compare the identifier to the list of policy identifiers (525, Fig. 5; page 13, lines 16-18), discard the message when the identifier does not match a policy identifier in the list (530, Fig. 5; page 13, lines 19-20), and implement an active version of the policy when the identifier matches a policy identifier in the list (540, Fig. 5; page 14, lines 1-2).

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-3, 5-7, 9, 10, 13, 14, 16, and 21 stand rejected under 35 U.S.C. § 102(e) as anticipated by Waclawsky (U.S. Patent No. 6,539,026).

B. Claims 4, 8, 11, 12, 15, 17-20, and 22-25 have been rejected under 35 U.S.C. § 103(a) as unpatentable over Waclawsky (U.S. Patent No. 6,539,026) in view of McCloghrie et al. (U.S. Patent No. 6,286,052).

VII. ARGUMENT

A. Rejection under 35 U.S.C. § 102(e) based on Waclawsky (U.S. Patent No. 6,539,026).

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). A proper rejection under 35 U.S.C. § 102 requires that a single reference teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 2 USPQ2d 1051 (Fed. Cir. 1987).

1. Claims 1, 2, 5, 6, and 9.

With the above principles in mind, Appellants' claim 1 is directed to a method that ensures policy coherence among a group of peer devices. The method includes detecting an addition of a new policy version, generating a message containing the newly added policy version in response to detecting the addition of the new policy version, and transferring the message to the peer devices. Waclawsky does not disclose or suggest this combination of features.

For example, Waclawsky does not disclose or suggest generating a message containing the newly added policy version in response to detecting the addition of the new policy version. The Examiner relies on col. 19, line 58, to col. 20, line 29, of Waclawsky for allegedly disclosing this feature (final Office Action, pg. 2). Appellants submit that this section of Waclawsky does not disclose or suggest the above feature of claim 1.

At col. 19, line 58, to col. 20, line 29, Waclawsky discloses:

Step 301 provides the ability to add or remove storage locations 259 from the series of storage locations 259-0 through 259-N each time the step is performed. As such, the invention allows the delay manager 201 to reconfigure itself if changes appear in the network policy 207. That is, the invention allows changes to be made at any time in the network policy 207, such as the addition or removal

of delay categories and/or data attributes. In response, a delay manager configured with the invention can periodically re-execute steps 300 through 302, as illustrated by the periodic re-execution line 310. Alternatively, re-execution of steps 301 through 303 can be triggered by the arrival or manual loading of new network policy information 207 into the data communications device 200. In this manner, the policy controller 250 in the delay manager(s) 201 in the data communications device(s) on network 100 periodically obtain the latest version of the network policy 207 from the network policy server 150 and can reconfigure the delay scheduler 251 and delay controller 252 via control commands 208 as previously described. This allows each data communications device 200 in an entire network to adapt to changes in a distributed network policy 207 with respect to the delay of data 205. Thus if new data types or data having new attributes becomes present on a network, the data communications devices 200 that use this invention can adapt to the new delay requirements without manually updating hardware or software within the devices 200.

This aspect of the invention thus ensures that a networked data communications device 200 is able to update itself with the latest network policy 207. Prior art network policy updates are typically performed by sending the network policy to each device by an affirmative act on the part of the network policy server 150. This invention eliminates the need to do this and places the burden for obtaining network policy updates on the data communication devices 200 themselves. As such, if there are hundreds or thousands of data communications devices 200 in the network, the load caused by network policy updates is distributed across each device.

This section of Waclawsky specifically discloses that policy controllers 250 in network devices 200 periodically obtain the latest version of network policy 207 from network policy server 150 (col. 20, lines 4-10). Waclawsky does not disclose or suggest, however, that policy controllers 250 obtain the latest version of network policy in response to detecting the addition of a new policy version, as required by claim 1. By stark contrast, Waclawsky specifically discloses that the obtaining of the latest version of network policy 207 occurs periodically. Moreover, this section of Waclawsky does not disclose or suggest that network policy server 150 (or any other device) generates a message containing a newly added policy version in response to detecting the addition of the new policy version, as required by claim 1. The Examiner has not logically explained how Waclawsky's disclosure that policy controllers 250 periodically obtain the latest version of network policy can reasonably be said to correspond to generating a message

containing the newly added policy version in response to detecting the addition of the new policy version, as required by claim 1. The Examiner has not pointed to any section of Waclawsky that discloses or suggests generating a message containing the newly added policy version in response to detecting the addition of the new policy version, as required by claim 1.

Since Waclawsky does not disclose generating a message containing the newly added policy version in response to detecting the addition of the new policy version, Waclawsky cannot disclose transferring the message to the peer devices, as also required by claim 1.

For at least the foregoing reasons, Appellants submit that the rejection of claim 1 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

2. Claims 3, 7, and 10.

Claim 3 recites determining whether a policy version has become newly active, generating a second message containing an indication of the newly active policy version, and sending the second message to the peer devices. Waclawsky does not disclose or suggest this combination of features.

At the outset, Appellants' note that claim 3 depends from claim 1 and, therefore, is not anticipated by Waclawsky for at least the reasons given above with respect to claim 1. Moreover, this claim is not anticipated by Waclawsky for reasons of its own.

The Examiner relies on col. 19, line 58, to col. 20, line 29, of Waclawsky for allegedly disclosing the features of claim 3 (final Office Action, pg. 3). Appellants disagree.

At col. 19, line 58, to col. 20, line 29, Waclawsky discloses:

Step 301 provides the ability to add or remove storage locations 259 from the series of storage locations 259-0 through 259-N each time the step is performed. As such, the invention allows the delay manager 201 to reconfigure itself if changes appear in the network policy 207. That is, the invention allows changes to be made at any time in the network policy 207, such as the addition or removal

of delay categories and/or data attributes. In response, a delay manager configured with the invention can periodically re-execute steps 300 through 302, as illustrated by the periodic re-execution line 310. Alternatively, re-execution of steps 301 through 303 can be triggered by the arrival or manual loading of new network policy information 207 into the data communications device 200. In this manner, the policy controller 250 in the delay manager(s) 201 in the data communications device(s) on network 100 periodically obtain the latest version of the network policy 207 from the network policy server 150 and can reconfigure the delay scheduler 251 and delay controller 252 via control commands 208 as previously described. This allows each data communications device 200 in an entire network to adapt to changes in a distributed network policy 207 with respect to the delay of data 205. Thus if new data types or data having new attributes becomes present on a network, the data communications devices 200 that use this invention can adapt to the new delay requirements without manually updating hardware or software within the devices 200.

This aspect of the invention thus ensures that a networked data communications device 200 is able to update itself with the latest network policy 207. Prior art network policy updates are typically performed by sending the network policy to each device by an affirmative act on the part of the network policy server 150. This invention eliminates the need to do this and places the burden for obtaining network policy updates on the data communication devices 200 themselves. As such, if there are hundreds or thousands of data communications devices 200 in the network, the load caused by network policy updates is distributed across each device.

This section of Waclawsky discloses the ability to reconfigure delay manager 201 of a network device 200 based on a network policy. This section of Waclawsky in no way discloses or suggests, however, determining whether a policy version has become active, generating a second message containing an indication of the newly active policy version, and sending the second message to the peer devices, as required by claim 3. The Examiner has not logically explained how the above section of Waclawsky can reasonably be construed to disclose the above features of claim 3.

The Examiner further alleges that "Waclawsky teaches the data communication device periodically determines whether another latest version (at time t1 which is later than time t) of network policy in the network policy server has become newly active. The network policy server generates another message that contains the another latest version of the network policy;

and sending the another message to the data communication device" and points to col. 19, line 58, to col. 20, line 29, of Waclawsky for support (final Office Action, pg. 5). Appellants submit that the Examiner has mischaracterized the disclosure of Waclawsky.

Contrary to the Examiner's allegation, Waclawsky does not disclose or suggest that the data communication device periodically determines whether another latest version of a network policy has become newly active. Instead, Waclawsky discloses that the data communication devices periodically obtain the latest version of network policy 207 (col. 20, lines 4-10).

Contrary to the Examiner's allegation, Waclawsky does not disclose or suggest that the data communication devices periodically obtaining the latest version of network policy 207 involves determining whether a policy version has become newly active, generating a second message containing an indication of the newly active policy version, or sending the second message to peer devices, as required by claim 3. The Examiner has not logically explained how the above section of Waclawsky can reasonably be construed to disclose the features of claim 3.

For at least the foregoing reasons, Appellants submit that the rejection of claim 3 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

3. Claim 13.

Independent claim 13 is directed to a method for distributing policies in a network having at least one anonymous policy server and at least one anonymous peer device. The method includes requesting a policy from the anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device. Waclawsky does not disclose or suggest this combination of features.

For example, Waclawsky does not disclose or suggest requesting a policy from an anonymous policy server. Waclawsky does not disclose or suggest that policy server 150 is an anonymous policy server, as required by claim 13. With respect to this feature, the Examiner alleges that "Waclawsky did not discuss device authentication prior to obtain the updates. Therefore, the network policy server and the devices are anonymous" (final Office Action, pg. 5). Appellants disagree.

The mere fact that Waclawsky does not disclose device authentication in no way discloses or suggests that network policy server 150 and network devices 200 are anonymous. In fact, Waclawsky specifically discloses that network devices 200 are access servers, routers, switches, hubs, bridges, gateways, proxy servers, concentrators, repeaters, and similar data transfer devices (col. 7, lines 2-6). Such network devices are typically not anonymous since anonymity of these devices could hinder the transfer of data through communications network 100. For example, routers typically know the identity of other routers in proximity to themselves so as to know how to route data through a network. The Examiner has not pointed to any section of Waclawsky that supports the allegation that network policy server 150 and network devices 200 are anonymous.

Since Waclawsky does not disclose or suggest that network policy server 150 and network devices 200 are anonymous, Waclawsky cannot disclose or suggest requesting a policy from an anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to an anonymous peer device, as required by claim 13.

Even assuming, for the sake of argument, that one skilled in the art could reasonably construe Waclawsky's network policy server 150 and network devices 200 as anonymous,

Appellants submit that Waclawsky does not disclose or suggest requesting a policy from an anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to an anonymous peer device, as required by claim 13. The Examiner did not address the combination of features recited in Appellants' claim 13 (see pp. 2-3 of final Office Action). Instead, the Examiner merely addressed the features of Appellants' claims 1-3. Appellants' claim 13 recites features not recited in claims 1-3. Therefore, a *prima facie* case of anticipation has not been established with respect to claim 13.

Nonetheless, Waclawsky discloses that a data communications device 200 can request policy updates from network server 150 when needed (col. 20, lines 18-29). Waclawsky in no way discloses or suggests, however, requesting a policy from an anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to an anonymous peer device, as required by claim 13.

For at least the foregoing reasons, Appellants submit that the rejection of claim 13 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

4. Claim 14.

Claim 14 recites that requesting a policy from the anonymous policy server includes generating, via the anonymous peer device, a policy request, where the policy request contains a policy identifier; and transferring the policy request to the anonymous policy server. Waclawsky does not disclose or suggest this combination of features.

At the outset, Appellants' note that claim 14 depends from claim 13 and, therefore, is not anticipated by Waclawsky for at least the reasons given above with respect to claim 13.

Moreover, this claim is not anticipated by Waclawsky for reasons of its own.

For example, Waclawsky does not disclose or suggest generating, via the anonymous peer device, a policy request, where the policy request contains a policy identifier. The Examiner has not addressed this feature in the final Office Action. Therefore, a *prima facie* case of anticipation has not been established with respect to claim 14.

Nonetheless, as set forth above, Waclawsky discloses that a data communications device 200 can request policy updates from network server 150 when needed (col. 20, lines 18-29).

Waclawsky does not disclose or suggest, however, that data communications device 200 is an anonymous peer device or that data communications device 200 generates a policy request that includes a policy identifier, as required by claim 14.

For at least the foregoing reasons, Appellants submit that the rejection of claim 14 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

5. Claim 16.

Claim 16 recites receiving, via the anonymous peer device, a policy; determining whether the received policy is the requested policy; discarding the received policy when the received policy is not the requested policy; and implementing the received policy when the received policy is the requested policy. Waclawsky does not disclose or suggest this combination of features.

At the outset, Appellants' note that claim 16 depends from claim 13 and, therefore, is not anticipated by Waclawsky for at least the reasons given above with respect to claim 13.

Moreover, this claim is not anticipated by Waclawsky for reasons of its own.

For example, Waclawsky does not disclose or suggest determining whether a received policy is the requested policy or discarding the received policy when the received policy is not the requested policy. The Examiner has not addressed this feature in the final Office Action. Therefore, a *prima facie* case of anticipation has not been established with respect to claim 16.

Nonetheless, as set forth above, Waclawsky discloses that a data communications device 200 can request policy updates from network server 150 when needed (col. 20, lines 18-29). Waclawsky does not disclose or suggest, however, that data communications device 200 is an anonymous peer device or that data communications device 200 determines whether a received policy is the requested policy or discards the received policy when the received policy is not the requested policy, as required by claim 16.

For at least the foregoing reasons, Appellants submit that the rejection of claim 16 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

6. Claim 21.

Independent claim 21 is directed to a computer-readable medium containing instructions for controlling at least one processor to perform a method that distributes policies in a network having a policy server and a peer device. The method includes receiving one or more requests, where each request indicates a policy of interest to the peer device; determining whether an active version of each of the policies exists; and transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device recites receiving, via the anonymous peer device, a policy. Waclawsky does not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the combination of features recited in Appellants' claim 21. Therefore, the Examiner has not established a *prima facie* case of anticipation with respect to claim 21.

Nonetheless, Waclawsky does not disclose or suggest determining whether an active version of each of the policies exists and transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device. To the contrary, Waclawsky discloses that policy controller 250 in network devices 200 periodically obtains the latest version of network policy 207 from network policy server 150 (col. 20, lines 4-10).

Since Waclawsky does not disclose or suggest all of the features of claim 21, Waclawsky does not anticipate claim 21.

For at least the foregoing reasons, Appellants submit that the rejection of claim 21 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

B. Rejection under 35 U.S.C. § 103(a) based on Waclawsky (U.S. Patent No. 6,539,026) and McCloghrie et al. (U.S. Patent No. 6,286,052).

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the Examiner must provide a factual basis to support the conclusion of obviousness. In re Warner, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967). Based upon the objective evidence of record, the Examiner is required to make the factual inquiries mandated by Graham v. John Deere Co., 86 S.Ct. 684, 383 U.S. 1, 148 USPQ 459 (1966). The Examiner is also required to explain how and why one having ordinary

skill in the art would have been realistically motivated to modify an applied reference and/or combine applied references to arrive at the claimed invention. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988).

In establishing the requisite motivation, it has been consistently held that the requisite motivation to support the conclusion of obviousness is not an abstract concept, but must stem from the prior art as a whole to impel one having ordinary skill in the art to modify a reference or to combine references with a reasonable expectation of successfully achieving some particular realistic objective. See, for example, Interconnect Planning Corp. v. Feil, 227 USPQ 543 (Fed. Cir. 1985). Consistent legal precedent admonishes against the indiscriminate combination of prior art references. Carella v. Starlight Archery, 804 F.2d 135, 231 USPQ 644 (Fed. Cir. 1986); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985).

1. Claims 4, 8, 11, and 12.

With the above principles in mind, Appellants' claim 4 depends indirectly from claim 1. The disclosure of McCloghrie et al. does not remedy the deficiencies in the disclosure of Waclawsky set forth above with respect to claim 1. Therefore, claim 4 is patentable over Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1. Moreover, this claim is patentable over Waclawsky and McCloghrie et al. for reasons of its own.

Claim 4 recites storing, in response to a policy version becoming newly active, an identifier of the newly active policy in an active policy database, where the active policy database stores a list of active policy identifiers. The Examiner admits that Waclawsky does not disclose these features and relies on col. 14, lines 25-44, of McCloghrie et al. for allegedly

disclosing the features of claim 4 (final Office Action, pp. 4-6). Appellants submit that McCloghrie et al. does not disclose the features of claim 4.

At col. 14, lines 25-44, McCloghrie et al. discloses:

The first policy binding 552a, for example, may contain an encoded copy of the source port identified by program 224 with the SetSourcePort() call 414a and stored at the respective traffic flow data structure 234. More specifically, message generator 230 loads policy identifier field 562a with the type or instance of the policy element (e.g., "source port"). In the preferred embodiment, this name is a Policy Identifier (PID) as specified in the Internet Engineering Task Force (IETF) draft document COPS Usage for Differentiated Services submitted by the Network Working Group, dated December 1998, and incorporated herein by reference in its entirety. A PID specifies a particular policy class (e.g., a type of policy data item) or policy instance (e.g., a particular instance of a given policy class) in a hierarchical arrangement. The Policy ID type field 560a contains a predefined value reflecting that field 562a contains information in PID format. Component 226 preferably includes a Policy Information Base (PIB) for use in deriving the particular policy identifiers, as described in COPS Usage for Differentiated Services.

This section of McCloghrie et al. discloses placing a Policy Identifier (PID) in a message. This section of McCloghrie et al. does not disclose or suggest, however, storing a PID of a newly active policy in an active policy database, in response to a policy version becoming newly active, where the active policy database stores a list of active policy identifiers, as required by claim 4.

Even assuming, for the sake of argument, that one skilled in the art could reasonably construe the disclosure of McCloghrie et al. to disclose the features of claim 4, Appellants submit that one skilled in the art would not have been motivated to combine the teachings of Waclawsky and McCloghrie et al. in the manner suggested by the Examiner, absent impermissible hindsight. With respect to motivation, the Examiner alleges that "[i]t would have been obvious ... to combine the teachings of Waclawsky and McCloghrie to stores a list of active policy identifiers in an active policy database because it would allow a device to be

configured for a particular services using active policies stored in the active policy database" (final Office Action, pp. 4 and 6). Appellants disagree.

The Examiner has not pointed to any section of Waclawsky or McCloghrie et al. to support the Examiner's motivation to combine McCloghrie et al. with Waclawsky. Waclawsky does not disclose or suggest an active policy database. The Examiner's motivation falls short of logically explaining why one would seek to incorporate an active policy database into the Waclawsky system. The Examiner's motivation is merely conclusory and insufficient for establishing a *prima facie* case of obviousness.

For at least the foregoing reasons, Appellants submit that the rejection of claim 4 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

2. Claims 15 and 20.

Claim 15 depends indirectly from claim 13. The disclosure of McCloghrie et al. does not remedy the deficiencies in the disclosure of Waclawsky set forth above with respect to claim 13. Therefore, claim 15 is patentable over Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 13. Moreover, this claim is patentable over Waclawsky and McCloghrie et al. for reasons of its own.

Claim 15 recites that the determining, via the anonymous policy server, whether an active version of the policy exists includes comparing the identifier in the policy request to a list of active policy identifiers. Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, do not disclose or suggest this feature.

The Examiner has not addressed the feature recited in claim 15. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation,

Appellants' claims 1-4 do not recite comparing the identifier in the policy request to a list of active policy identifiers, as required by claim 15. Since the Examiner has not addressed the feature of claim 15, a *prima facie* case of obviousness has not been established with respect to claim 15.

For at least the foregoing reasons, Appellants submit that the rejection of claim 15 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

3. Claims 17-19.

Claim 17 is directed to network that includes at least one anonymous peer device and at least one anonymous policy server. The at least one anonymous peer device is configured to request a policy from at least one anonymous policy server, determine whether a received policy is of a desired policy class, and implement the received policy when the received policy is an active policy of the desired policy class. The at least one anonymous policy server is configured to receive the request from the at least one anonymous peer device, determine whether any version of the policy requested exists, and transfer all versions of the policy to the peer device, indicating the active version, if any version is determined to exist. Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, Waclawsky and McCloghrie et al. do not disclose or suggest at least one anonymous peer device and at least one anonymous policy server. As set forth above, Waclawsky does not disclose or suggest that policy server 150 is an anonymous policy server. Moreover, Waclawsky does not disclose or suggest that network devices 200 are anonymous peer devices. McCloghrie et al. discloses a policy server 216, but does not disclose or suggest

that policy server 216 is an anonymous policy server. Moreover, McCloghrie et al. does not disclose or suggest at least one anonymous peer device.

As discussed above, the Examiner alleges that "Waclawsky did not discuss device authentication prior to obtain the updates. Therefore, the network policy server and the devices are anonymous" (final Office Action, pg. 5). Appellants disagree.

The mere fact that Waclawsky does not disclose device authentication in no way discloses or suggests that network policy server 150 and network devices 200 are anonymous. In fact, Waclawsky specifically discloses that network devices 200 are access servers, routers, switches, hubs, bridges, gateways, proxy servers, concentrators, repeaters, and similar data transfer devices (col. 7, lines 2-6). Such network devices are typically not anonymous since anonymity of these devices could hinder the transfer of data through communications network 100. For example, routers typically know the identity of other routers in proximity to themselves so as to know how to route data through a network. The Examiner has not pointed to any section of Waclawsky that supports the allegation that network policy server 150 and network devices 200 are anonymous.

Even assuming, for the sake of argument, that Waclawsky's network policy server 150 and network devices 200 could be considered anonymous, Waclawsky and McCloghrie et al. do not disclose features of Appellants' claim 17. For example, Waclawsky and McCloghrie et al. do not disclose or suggest at least one anonymous peer device that is configured to determine whether a received policy is of a desired policy class and implement the received policy when the received policy is an active policy of the desired policy class or at least one anonymous policy server that is configured to determine whether any version of a requested policy exists and transfer all versions of the policy to the peer device, indicating the active version if any version is determined to exist, as required by claim 17.

The Examiner has not addressed the features of claim 17. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above features of claim 17. Since the Examiner has not addressed the above features of claim 17, a *prima facie* case of obviousness has not been established with respect to claim 17.

For at least the foregoing reasons, Appellants submit that the rejection of claim 17 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

4. Claim 22.

Independent claim 22 recites a computer-readable medium having a database structure that includes a policy identification field that stores an identifier of a policy, a version field that stores an identifier of a policy version, and a policy content field that stores a content of a policy. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 22. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above features of claim 22. Since the Examiner has not addressed the above features of claim 22, a *prima facie* case of obviousness has not been established with respect to claim 22.

For at least the foregoing reasons, Appellants submit that the rejection of claim 22 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

5. Claim 23.

Independent claim 23 recites a computer-readable medium having a database structure that includes a policy identification field that stores an identifier of a policy, and a version field that stores an identifier of an active policy version. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 23. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above features of claim 23. Since the Examiner has not addressed the above features of claim 23, a *prima facie* case of obviousness has not been established with respect to claim 23.

For at least the foregoing reasons, Appellants submit that the rejection of claim 23 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

6. Claim 24.

Independent claim 24 is directed to a method for implementing policies. The method includes receiving a message, where the message contains an identifier and one or more versions of a policy; determining whether the identifier is in a list of policy identifiers; discarding the message when the identifier is absent from the list; and implementing an active version of the one or more policies when the identifier is present in the list. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 24. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above

combination of features of claim 24. Since the Examiner has not addressed the above features of claim 24, a *prima facie* case of obviousness has not been established with respect to claim 24.

For at least the foregoing reasons, Appellants submit that the rejection of claim 24 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

7. Claim 25.

Independent claim 25 is directed to a system for implementing policies. The system includes a memory and a processor. The memory is configured to store instructions and an active policy database, where the active policy database contains a list of policy identifiers. The processor is configured to execute the instructions to receive a message, where the message contains an identifier and one or more versions of a policy, compare the identifier to the list of policy identifiers, discard the message when the identifier does not match a policy identifier in the list, and implement an active version of the policy when the identifier matches a policy identifier in the list. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 25. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above combination of features of claim 25. Since the Examiner has not addressed the above features of claim 25, a *prima facie* case of obviousness has not been established with respect to claim 25.

For at least the foregoing reasons, Appellants submit that the rejection of claim 25 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

Application No.: 09/658207

Docket No.: BBNT-P01-109

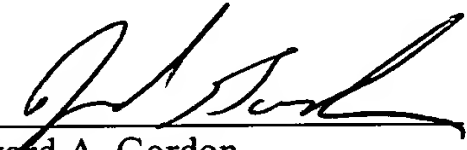
VIII. CONCLUSION

In view of the foregoing arguments, Appellants respectfully solicit the Honorable Board to reverse the Examiner's rejections of claims 1-25 under 35 U.S.C. §§ 102 and 103.

Applicant believes no fee is due with this response other than as reflected on the enclosed fee transmittal. However, if a fee is due, please charge our Deposit Account No. 18-1945, under Order No. BBNT-P01-109 from which the undersigned is authorized to draw.

Dated: December 17, 2004

Respectfully submitted,

By 
Edward A. Gordon
Registration No.: 54,130
ROPES & GRAY LLP
One International Place
Boston, 02110-2624
(617) 951-7000
(617) 951-7050 (Fax)
Attorneys/Agents For Applicant

CLAIM APPENDIX

1. A method that ensures policy coherence among a group of peer devices, comprising:
 - detecting an addition of a new policy version;
 - generating a message containing the newly added policy version in response to detecting the addition of the new policy version; and
 - transferring the message to the peer devices.
2. The method of claim 1 wherein the newly added policy version is a policy that relates to at least one of system administration, system security, command and control, and courses of action.
3. The method of claim 1 further comprising:
 - determining whether a policy version has become newly active;
 - generating a second message containing an indication of the newly active policy version; and
 - sending the second message to the peer devices.
4. The method of claim 3 further comprising:
 - storing, in response to a policy version becoming newly active, an identifier of the newly active policy in an active policy database, the active policy database storing a list of active policy identifiers.

5. A system that ensures policy coherence among a group of peer devices, comprising:
 - means for detecting an addition of one or more new policy versions;
 - means for generating a message containing the newly added one or more policy versions in response to detecting the addition of one or more policy versions; and
 - means for transferring the message to the peer devices.
6. A computer-readable medium containing instructions for controlling at least one processor to perform a method that ensures policy coherence among a group of peer devices, the method comprising:
 - determining whether a policy has been added;
 - generating, in response to a policy being added, a message containing the added policy; and
 - sending the message to the peer devices.
7. The computer-readable medium of claim 6 wherein the method further comprises:
 - determining whether a version of one of a group of policies has become active;
 - generating a second message containing the active version;
 - transferring the second message to the peer devices.
8. The computer-readable medium of claim 7 wherein the method further comprises:
 - storing an identifier of the newly active policy in an active policy database, the active policy database including a list of active policy identifiers.

9. A policy server comprising:
 - a memory configured to store instructions; and
 - a processor configured to execute the instructions to determine whether one or more policy versions have been added, generate, in response to a policy version being added, a message containing the added policy version, and transfer the message to a group of peer devices.
10. The policy server of claim 9 wherein the processor is further configured to:
 - detect a policy version becoming newly active,
 - generate, in response to the detecting, a second message containing the newly active policy version, and
 - transmit the second message to the group of peer devices.
11. The policy server of claim 10 wherein the memory is further configured to:
 - store an active policy database containing a list of identifiers of active policies.
12. The policy server of claim 11 wherein the processor is further configured to:
 - store, in response to a policy becoming active, an identifier of the newly active policy in the active policy database.
13. A method for distributing policies in a network having at least one anonymous policy server and at least one anonymous peer device, comprising:
 - requesting a policy from the anonymous policy server;

determining, via the anonymous policy server, whether an active version of the policy exists; and

transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device.

14. The method of claim 13 wherein the requesting includes:

generating, via the anonymous peer device, a policy request, the policy request containing a policy identifier; and

transferring the policy request to the anonymous policy server.

15. The method of claim 14 wherein the determining includes:

comparing the identifier in the policy request to a list of active policy identifiers.

16. The method of claim 13 further comprising:

receiving, via the anonymous peer device, a policy;

determining whether the received policy is the requested policy;

discarding the received policy when the received policy is not the requested policy; and

implementing the received policy when the received policy is the requested policy.

17. A network comprising:

at least one anonymous peer device configured to:

request a policy from at least one anonymous policy server,

determine whether a received policy is of a desired policy class, and
implement the received policy when the received policy is an active
policy of the desired policy class; and

at least one anonymous policy server configured to:

receive the request from the at least one anonymous peer device,
determine whether any version of the policy requested exists, and
transfer all versions of the policy to the peer device, indicating the active
version, if any version is determined to exist.

18. The network of claim 17 wherein the at least one anonymous peer device is
further configured to:

discard the received policy when the received policy is not of the requested policy
class.

19. The network of claim 17 wherein, when requesting, the at least one anonymous
peer device is configured to:

generate a policy request, the policy request containing an identifier that identifies
the requested policy, and

transfer the policy request to the at least one anonymous policy server.

20. The network of claim 18 wherein, when determining, the at least one anonymous
policy server is configured to:

compare the identifier in the policy request to a list of active policy identifiers.

21. A computer-readable medium containing instructions for controlling at least one processor to perform a method that distributes policies in a network having a policy server and a peer device, the method comprising:

receiving one or more requests, each request indicating a policy of interest to the peer device;

determining whether an active version of each of the policies exists; and

transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device.

22. A computer-readable medium having a database structure comprising:

a policy identification field that stores an identifier of a policy;

a version field that stores an identifier of a policy version; and

a policy content field that stores a content of a policy.

23. A computer-readable medium having a database structure comprising:

a policy identification field that stores an identifier of a policy; and

a version field that stores an identifier of an active policy version.

24. A method for implementing policies, comprising:

receiving a message, the message containing an identifier and one or more versions of a policy;

determining whether the identifier is in a list of policy identifiers;

discarding the message when the identifier is absent from the list; and

implementing an active version of the one or more policies when the identifier is present in the list.

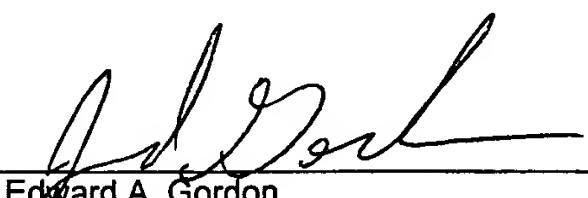
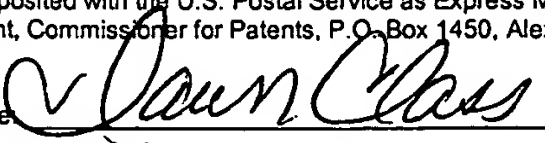
25. A system for implementing policies comprising:

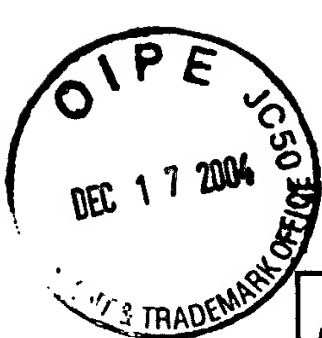
a memory configured to store instructions and an active policy database, the active policy database containing a list of policy identifiers; and

a processor configured to execute the instructions to receive a message, the message containing an identifier and one or more versions of a policy, compare the identifier to the list of policy identifiers, discard the message when the identifier does not match a policy identifier in the list, and implement an active version of the policy when the identifier matches a policy identifier in the list.



COPY

TRANSMITTAL OF APPEAL BRIEF			Docket No. BBNT-P01-109	
In re Application of: Donaghey et al.				
Application No. 09/658207	Filing Date September 8, 2000	Examiner L. H. Luu	Group Art Unit 2141	
Invention: SYSTEM AND METHOD FOR SELECTING AND DISSEMINATING POLICIES				
<u>TO THE COMMISSIONER OF PATENTS:</u>				
Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: <u>October 18, 2004</u> .				
The fee for filing this Appeal Brief is <u>\$ 500.00</u> .				
<input checked="" type="checkbox"/> Large Entity <input type="checkbox"/> Small Entity				
<input type="checkbox"/> A petition for extension of time is also enclosed.				
The fee for the extension of time is _____.				
<input type="checkbox"/> A check in the amount of _____ is enclosed.				
<input checked="" type="checkbox"/> Charge the amount of the fee to Deposit Account No. <u>18-1945</u> . This sheet is submitted in duplicate.				
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.				
<input checked="" type="checkbox"/> The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. <u>18-1945</u> . This sheet is submitted in duplicate.				
 Edward A. Gordon Attorney Reg. No. : 54,130 ROPES & GRAY LLP One International Place Boston, 02110-2624 (617) 951-7066			Dated: <u>December 17, 2004</u>	
<p>I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 543609163 US, in an envelope addressed to: MS Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.</p> <p>Dated: <u>12/17/04</u> Signature:  (Dawn Marie Class)</p>				



COPY

PTO/SB/17 (12-04)

Approved for use through 7/31/2006. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no person are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 12/08/2004. Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818). FEE TRANSMITTAL For FY 2005		Complete if Known	
		Application Number	09/658207
		Filing Date	September 8, 2000
		First Named Inventor	Robert J. Donaghey
		Examiner Name	L. H. Luu
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27	Art Unit	2141	
TOTAL AMOUNT OF PAYMENT	(\$) 500.00	Attorney Docket No.	BBNT-P01-109

METHOD OF PAYMENT (check all that apply)	
<input type="checkbox"/> Check	<input type="checkbox"/> Credit Card
<input type="checkbox"/> Money Order	<input type="checkbox"/> None
<input type="checkbox"/> Other (please identify): _____	
<input checked="" type="checkbox"/> Deposit Account	Deposit Account Number: 18-1945 Deposit Account Name: Ropes & Gray LLP
For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)	
<input checked="" type="checkbox"/> Charge fee(s) indicated below	<input type="checkbox"/> Charge fee(s) indicated below, except for the filing fee
<input checked="" type="checkbox"/> Charge any additional fee(s) or any underpayment of fee(s) under 37 CFR 1.16 and 1.17	<input checked="" type="checkbox"/> Credit any overpayments

FEE CALCULATION							
1. BASIC FILING, SEARCH, AND EXAMINATION FEES							
	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		<u>Small Entity</u>		<u>Small Entity</u>		<u>Small Entity</u>	
Application Type	Fee (\$)	Fee (\$)	Fee (\$)	Fee (\$)	Fee (\$)	Fee (\$)	Fees Paid (\$)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	
2. EXCESS CLAIM FEES							
						<u>Small Entity</u>	
						Fee (\$)	Fee (\$)
Fee Description							
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent						50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent						200	100
Multiple dependent claims						360	180
Total Claims		Extra Claims	Fee (\$)	Fee Paid (\$)	Multiple Dependent Claims		
_____ - = _____		x _____	= _____		Fee (\$) Fee Paid (\$)		
Indep. Claims		Extra Claims	Fee (\$)	Fee Paid (\$)			
_____ - = _____		x _____	= _____				
3. APPLICATION SIZE FEE							
If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).							
Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof			Fee (\$)	Fee Paid (\$)	
_____ - 100 = _____	/50	_____ (round up to a whole number) x _____			= _____		
4. OTHER FEE(S)							
Non-English Specification, \$130 fee (no small entity discount)							
Other: 1402 Filing a brief in support of an appeal						500.00	

SUBMITTED BY			
Signature		Registration No. (Attorney/Agent)	54,130
Name (Print/Type)	Edward A. Gordon	Telephone	(617) 951-7066
		Date	December 17, 2004

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 543609163 US, in an envelope addressed to: MS Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.		
Dated: 12/17/04	Signature:	(Dawn Class)



I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 543609163 US, in an envelope addressed to: MS Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: 12/17/04 Signature: Dawn Class
(Dawn Class)

Docket No.: BBNT-P01-109
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Donaghey et al.

Application No.: 09/658207

Confirmation No.: 3500

Filed: September 8, 2000

Art Unit: 2141

For: SYSTEM AND METHOD FOR SELECTING
AND DISSEMINATING POLICIES

Examiner: L. H. Luu

APPEAL BRIEF

COPY

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in response to the final Office Action, dated April 20, 2004, and in support of the Notice of Appeal, filed October 18, 2004.

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is BBNT Solutions LLC.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

Appellants are unaware of any related appeals, interferences or judicial proceedings.

III. STATUS OF CLAIMS

Claims 1-25 are pending in this application.

Claims 1-3, 5-7, 9, 10, 13, 14, 16, and 21 have been rejected under 35 U.S.C. § 102(e) as anticipated by Waclawsky (U.S. Patent No. 6,539,026).

Claims 4, 8, 11, 12, 15, 17-20, and 22-25 have been rejected under 35 U.S.C. § 103(a) as unpatentable over Waclawsky in view of McCloghrie et al. (U.S. Patent No. 6,286,052).

Claims 1-3, 5-7, 9, 10, 13, 14, 16, and 21 have been rejected under 35 U.S.C. § 102(e) as anticipated by Waclawsky (U.S. Patent No. 6,539,026).

Claims 4, 8, 11, 12, 15, 17-20, and 22-25 have been rejected under 35 U.S.C. § 103(a) as unpatentable over Waclawsky in view of McCloghrie et al. (U.S. Patent No. 6,286,052).

Claims 1-25 are the subject of the present appeal. These claims are reproduced in the Claim Appendix of this Appeal Brief.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final Office Action, dated April 20, 2004.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In the paragraphs that follow, each of the independent claims that is involved in this appeal will be recited followed in parenthesis by examples of where support can be found in the specification and drawings.

Claim 1 recites a method that ensures policy coherence among a group of peer devices (110), comprising: detecting an addition of a new policy version (650, Fig. 6B; page 15, lines 18-20); generating a message containing the newly added policy version in response to detecting the addition of the new policy version (655, 665, Fig. 6B; page 15, line 20, to page 16, line 7); and transferring the message to the peer devices (670, Fig. 6B; page 16, lines 7-8).

Claim 5 recites a system that ensures policy coherence among a group of peer devices, comprising: means for detecting an addition of one or more new policy versions (120, Fig. 1; 650, Fig. 6B; page 15, lines 18-20); means for generating a message containing the newly added one or more policy versions in response to detecting the addition of one or more policy versions

(120, Fig. 1; 655, 665, Fig. 6B; page 15, line 20, to page 16, line 7); and means for transferring the message to the peer devices (120, Fig. 1; 670, Fig. 6B; page 16, lines 7-8).

Claim 6 recites a computer-readable medium (206, Fig. 2) containing instructions for controlling at least one processor (204, Fig. 2) to perform a method that ensures policy coherence among a group of peer devices, the method comprising: determining whether a policy has been added (650, Fig. 6B; page 15, lines 18-20); generating, in response to a policy being added, a message containing the added policy (655, 665, Fig. 6B; page 15, line 20, to page 16, line 7); and sending the message to the peer devices (670, Fig. 6B; page 16, lines 7-8).

Claim 9 recites a policy server (120, Fig. 1) comprising: a memory configured to store instructions (206, Fig. 2; page 8, lines 16-20); and a processor (204, Fig. 2) configured to execute the instructions to determine whether one or more policy versions have been added (650, Fig. 6B; page 15, lines 18-20), generate, in response to a policy version being added, a message containing the added policy version (655, 665, Fig. 6B; page 15, line 20, to page 16, line 7), and transfer the message to a group of peer devices (670, Fig. 6B; page 16, lines 7-8).

Claim 13 recites a method for distributing policies in a network having at least one anonymous policy server (120, Fig. 1) and at least one anonymous peer device (110, Fig. 1), comprising: requesting a policy from the anonymous policy server (505, 510, Fig. 5; page 13, lines 1-11); determining, via the anonymous policy server, whether an active version of the policy exists (605-615, Fig. 6A; page 14, lines 5-16); and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device (630, 635, Fig. 6A; page 14, line 19, to page 15, line 6).

Claim 17 recites a network comprising: at least one anonymous peer device (110, Fig. 1) configured to: request a policy from at least one anonymous policy server (505, 510, Fig. 5; page 13, lines 1-11), determine whether a received policy is of a desired policy class (515-525, Fig. 5;

page 13, lines 12-18), and implement the received policy when the received policy is an active policy of the desired policy class (540, Fig. 5; page 13, line 20, to page 14, line 3); and at least one anonymous policy server (120, Fig. 1) configured to: receive the request from the at least one anonymous peer device (610, Fig. 6A; page 14, lines 5-9), determine whether any version of the policy requested exists (615, Fig. 6A; page 14, lines 9-16), and transfer all versions of the policy to the peer device, indicating the active version, if any version is determined to exist (620, 630, 635, Fig. 6A; page 14, line 19, to page 15, line 6).

Claim 21 recites a computer-readable medium (206, Fig. 2) containing instructions for controlling at least one processor (204, Fig. 2) to perform a method that distributes policies in a network having a policy server and a peer device, the method comprising: receiving one or more requests, each request indicating a policy of interest to the peer device (610, Fig. 6A; page 14, lines 5-9); determining whether an active version of each of the policies exists (615, Fig. 6A; page 14, lines 9-16); and transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device (620, 630, 635, Fig. 6A; page 14, lines 19-22).

Claim 22 recites a computer-readable medium having a database structure (300, Fig. 3A) comprising: a policy identification field that stores an identifier of a policy (310, Fig. 3A; page 9, lines 17-19); a version field that stores an identifier of a policy version (320, Fig. 3A; page 10, lines 1-2); and a policy content field that stores a content of a policy (350, Fig. 3A; page 10, lines 8-9).

Claim 23 recites a computer-readable medium having a database structure (301, Fig. 3B) comprising: a policy identification field that stores an identifier of a policy (360, Fig. 3B; page 10, lines 14-15); and a version field that stores an identifier of an active policy version (370, Fig. 3B; page 10, lines 15-17).

Claim 24 recites a method for implementing policies, comprising: receiving a message, the message containing an identifier and one or more versions of a policy (520, Fig. 5; page 13, lines 14-16); determining whether the identifier is in a list of policy identifiers (525, Fig. 5; page 13, lines 14-18); discarding the message when the identifier is absent from the list (530, Fig. 5; page 13, lines 19-20); and implementing an active version of the one or more policies when the identifier is present in the list (540, Fig. 5; page 13, line 20, to page 14, line 2).

Claim 25 recites a system for implementing policies comprising: a memory (430, Fig. 4) configured to store instructions and an active policy database, the active policy database containing a list of policy identifiers (page 12, lines 1-10); and a processor (420, Fig. 4) configured to execute the instructions to receive a message, the message containing an identifier and one or more versions of a policy (520, Fig. 5; page 13, lines 14-16), compare the identifier to the list of policy identifiers (525, Fig. 5; page 13, lines 16-18), discard the message when the identifier does not match a policy identifier in the list (530, Fig. 5; page 13, lines 19-20), and implement an active version of the policy when the identifier matches a policy identifier in the list (540, Fig. 5; page 14, lines 1-2).

VI. GROUND S OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-3, 5-7, 9, 10, 13, 14, 16, and 21 stand rejected under 35 U.S.C. § 102(e) as anticipated by Waclawsky (U.S. Patent No. 6,539,026).

B. Claims 4, 8, 11, 12, 15, 17-20, and 22-25 have been rejected under 35 U.S.C. § 103(a) as unpatentable over Waclawsky (U.S. Patent No. 6,539,026) in view of McCloghrie et al. (U.S. Patent No. 6,286,052).

VII. ARGUMENT

A. Rejection under 35 U.S.C. § 102(e) based on Waclawsky (U.S. Patent No. 6,539,026).

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). A proper rejection under 35 U.S.C. § 102 requires that a single reference teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 2 USPQ2d 1051 (Fed. Cir. 1987).

1. Claims 1, 2, 5, 6, and 9.

With the above principles in mind, Appellants' claim 1 is directed to a method that ensures policy coherence among a group of peer devices. The method includes detecting an addition of a new policy version, generating a message containing the newly added policy version in response to detecting the addition of the new policy version, and transferring the message to the peer devices. Waclawsky does not disclose or suggest this combination of features.

For example, Waclawsky does not disclose or suggest generating a message containing the newly added policy version in response to detecting the addition of the new policy version. The Examiner relies on col. 19, line 58, to col. 20, line 29, of Waclawsky for allegedly disclosing this feature (final Office Action, pg. 2). Appellants submit that this section of Waclawsky does not disclose or suggest the above feature of claim 1.

At col. 19, line 58, to col. 20, line 29, Waclawsky discloses:

Step 301 provides the ability to add or remove storage locations 259 from the series of storage locations 259-0 through 259-N each time the step is performed. As such, the invention allows the delay manager 201 to reconfigure itself if changes appear in the network policy 207. That is, the invention allows changes to be made at any time in the network policy 207, such as the addition or removal

of delay categories and/or data attributes. In response, a delay manager configured with the invention can periodically re-execute steps 300 through 302, as illustrated by the periodic re-execution line 310. Alternatively, re-execution of steps 301 through 303 can be triggered by the arrival or manual loading of new network policy information 207 into the data communications device 200. In this manner, the policy controller 250 in the delay manager(s) 201 in the data communications device(s) on network 100 periodically obtain the latest version of the network policy 207 from the network policy server 150 and can reconfigure the delay scheduler 251 and delay controller 252 via control commands 208 as previously described. This allows each data communications device 200 in an entire network to adapt to changes in a distributed network policy 207 with respect to the delay of data 205. Thus if new data types or data having new attributes becomes present on a network, the data communications devices 200 that use this invention can adapt to the new delay requirements without manually updating hardware or software within the devices 200.

This aspect of the invention thus ensures that a networked data communications device 200 is able to update itself with the latest network policy 207. Prior art network policy updates are typically performed by sending the network policy to each device by an affirmative act on the part of the network policy server 150. This invention eliminates the need to do this and places the burden for obtaining network policy updates on the data communication devices 200 themselves. As such, if there are hundreds or thousands of data communications devices 200 in the network, the load caused by network policy updates is distributed across each device.

This section of Waclawsky specifically discloses that policy controllers 250 in network devices 200 periodically obtain the latest version of network policy 207 from network policy server 150 (col. 20, lines 4-10). Waclawsky does not disclose or suggest, however, that policy controllers 250 obtain the latest version of network policy in response to detecting the addition of a new policy version, as required by claim 1. By stark contrast, Waclawsky specifically discloses that the obtaining of the latest version of network policy 207 occurs periodically. Moreover, this section of Waclawsky does not disclose or suggest that network policy server 150 (or any other device) generates a message containing a newly added policy version in response to detecting the addition of the new policy version, as required by claim 1. The Examiner has not logically explained how Waclawsky's disclosure that policy controllers 250 periodically obtain the latest version of network policy can reasonably be said to correspond to generating a message

containing the newly added policy version in response to detecting the addition of the new policy version, as required by claim 1. The Examiner has not pointed to any section of Waclawsky that discloses or suggests generating a message containing the newly added policy version in response to detecting the addition of the new policy version, as required by claim 1.

Since Waclawsky does not disclose generating a message containing the newly added policy version in response to detecting the addition of the new policy version, Waclawsky cannot disclose transferring the message to the peer devices, as also required by claim 1.

For at least the foregoing reasons, Appellants submit that the rejection of claim 1 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

2. Claims 3, 7, and 10.

Claim 3 recites determining whether a policy version has become newly active, generating a second message containing an indication of the newly active policy version, and sending the second message to the peer devices. Waclawsky does not disclose or suggest this combination of features.

At the outset, Appellants' note that claim 3 depends from claim 1 and, therefore, is not anticipated by Waclawsky for at least the reasons given above with respect to claim 1. Moreover, this claim is not anticipated by Waclawsky for reasons of its own.

The Examiner relies on col. 19, line 58, to col. 20, line 29, of Waclawsky for allegedly disclosing the features of claim 3 (final Office Action, pg. 3). Appellants disagree.

At col. 19, line 58, to col. 20, line 29, Waclawsky discloses:

Step 301 provides the ability to add or remove storage locations 259 from the series of storage locations 259-0 through 259-N each time the step is performed. As such, the invention allows the delay manager 201 to reconfigure itself if changes appear in the network policy 207. That is, the invention allows changes to be made at any time in the network policy 207, such as the addition or removal

of delay categories and/or data attributes. In response, a delay manager configured with the invention can periodically re-execute steps 300 through 302, as illustrated by the periodic re-execution line 310. Alternatively, re-execution of steps 301 through 303 can be triggered by the arrival or manual loading of new network policy information 207 into the data communications device 200. In this manner, the policy controller 250 in the delay manager(s) 201 in the data communications device(s) on network 100 periodically obtain the latest version of the network policy 207 from the network policy server 150 and can reconfigure the delay scheduler 251 and delay controller 252 via control commands 208 as previously described. This allows each data communications device 200 in an entire network to adapt to changes in a distributed network policy 207 with respect to the delay of data 205. Thus if new data types or data having new attributes becomes present on a network, the data communications devices 200 that use this invention can adapt to the new delay requirements without manually updating hardware or software within the devices 200.

This aspect of the invention thus ensures that a networked data communications device 200 is able to update itself with the latest network policy 207. Prior art network policy updates are typically performed by sending the network policy to each device by an affirmative act on the part of the network policy server 150. This invention eliminates the need to do this and places the burden for obtaining network policy updates on the data communication devices 200 themselves. As such, if there are hundreds or thousands of data communications devices 200 in the network, the load caused by network policy updates is distributed across each device.

This section of Waclawsky discloses the ability to reconfigure delay manager 201 of a network device 200 based on a network policy. This section of Waclawsky in no way discloses or suggests, however, determining whether a policy version has become active, generating a second message containing an indication of the newly active policy version, and sending the second message to the peer devices, as required by claim 3. The Examiner has not logically explained how the above section of Waclawsky can reasonably be construed to disclose the above features of claim 3.

The Examiner further alleges that "Waclawsky teaches the data communication device periodically determines whether another latest version (at time t1 which is later than time t) of network policy in the network policy server has become newly active. The network policy server generates another message that contains the another latest version of the network policy;

and sending the another message to the data communication device" and points to col. 19, line 58, to col. 20, line 29, of Waclawsky for support (final Office Action, pg. 5). Appellants submit that the Examiner has mischaracterized the disclosure of Waclawsky.

Contrary to the Examiner's allegation, Waclawsky does not disclose or suggest that the data communication device periodically determines whether another latest version of a network policy has become newly active. Instead, Waclawsky discloses that the data communication devices periodically obtain the latest version of network policy 207 (col. 20, lines 4-10).

Contrary to the Examiner's allegation, Waclawsky does not disclose or suggest that the data communication devices periodically obtaining the latest version of network policy 207 involves determining whether a policy version has become newly active, generating a second message containing an indication of the newly active policy version, or sending the second message to peer devices, as required by claim 3. The Examiner has not logically explained how the above section of Waclawsky can reasonably be construed to disclose the features of claim 3.

For at least the foregoing reasons, Appellants submit that the rejection of claim 3 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

3. Claim 13.

Independent claim 13 is directed to a method for distributing policies in a network having at least one anonymous policy server and at least one anonymous peer device. The method includes requesting a policy from the anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device. Waclawsky does not disclose or suggest this combination of features.

For example, Waclawsky does not disclose or suggest requesting a policy from an anonymous policy server. Waclawsky does not disclose or suggest that policy server 150 is an anonymous policy server, as required by claim 13. With respect to this feature, the Examiner alleges that "Waclawsky did not discuss device authentication prior to obtain the updates. Therefore, the network policy server and the devices are anonymous" (final Office Action, pg. 5). Appellants disagree.

The mere fact that Waclawsky does not disclose device authentication in no way discloses or suggests that network policy server 150 and network devices 200 are anonymous. In fact, Waclawsky specifically discloses that network devices 200 are access servers, routers, switches, hubs, bridges, gateways, proxy servers, concentrators, repeaters, and similar data transfer devices (col. 7, lines 2-6). Such network devices are typically not anonymous since anonymity of these devices could hinder the transfer of data through communications network 100. For example, routers typically know the identity of other routers in proximity to themselves so as to know how to route data through a network. The Examiner has not pointed to any section of Waclawsky that supports the allegation that network policy server 150 and network devices 200 are anonymous.

Since Waclawsky does not disclose or suggest that network policy server 150 and network devices 200 are anonymous, Waclawsky cannot disclose or suggest requesting a policy from an anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to an anonymous peer device, as required by claim 13.

Even assuming, for the sake of argument, that one skilled in the art could reasonably construe Waclawsky's network policy server 150 and network devices 200 as anonymous,

Appellants submit that Waclawsky does not disclose or suggest requesting a policy from an anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to an anonymous peer device, as required by claim 13. The Examiner did not address the combination of features recited in Appellants' claim 13 (see pp. 2-3 of final Office Action). Instead, the Examiner merely addressed the features of Appellants' claims 1-3. Appellants' claim 13 recites features not recited in claims 1-3. Therefore, a *prima facie* case of anticipation has not been established with respect to claim 13.

Nonetheless, Waclawsky discloses that a data communications device 200 can request policy updates from network server 150 when needed (col. 20, lines 18-29). Waclawsky in no way discloses or suggests, however, requesting a policy from an anonymous policy server; determining, via the anonymous policy server, whether an active version of the policy exists; and transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to an anonymous peer device, as required by claim 13.

For at least the foregoing reasons, Appellants submit that the rejection of claim 13 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

4. Claim 14.

Claim 14 recites that requesting a policy from the anonymous policy server includes generating, via the anonymous peer device, a policy request, where the policy request contains a policy identifier; and transferring the policy request to the anonymous policy server. Waclawsky does not disclose or suggest this combination of features.

At the outset, Appellants' note that claim 14 depends from claim 13 and, therefore, is not anticipated by Waclawsky for at least the reasons given above with respect to claim 13.

Moreover, this claim is not anticipated by Waclawsky for reasons of its own.

For example, Waclawsky does not disclose or suggest generating, via the anonymous peer device, a policy request, where the policy request contains a policy identifier. The Examiner has not addressed this feature in the final Office Action. Therefore, a *prima facie* case of anticipation has not been established with respect to claim 14.

Nonetheless, as set forth above, Waclawsky discloses that a data communications device 200 can request policy updates from network server 150 when needed (col. 20, lines 18-29). Waclawsky does not disclose or suggest, however, that data communications device 200 is an anonymous peer device or that data communications device 200 generates a policy request that includes a policy identifier, as required by claim 14.

For at least the foregoing reasons, Appellants submit that the rejection of claim 14 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

5. Claim 16.

Claim 16 recites receiving, via the anonymous peer device, a policy; determining whether the received policy is the requested policy; discarding the received policy when the received policy is not the requested policy; and implementing the received policy when the received policy is the requested policy. Waclawsky does not disclose or suggest this combination of features.

At the outset, Appellants' note that claim 16 depends from claim 13 and, therefore, is not anticipated by Waclawsky for at least the reasons given above with respect to claim 13. Moreover, this claim is not anticipated by Waclawsky for reasons of its own.

For example, Waclawsky does not disclose or suggest determining whether a received policy is the requested policy or discarding the received policy when the received policy is not the requested policy. The Examiner has not addressed this feature in the final Office Action. Therefore, a *prima facie* case of anticipation has not been established with respect to claim 16.

Nonetheless, as set forth above, Waclawsky discloses that a data communications device 200 can request policy updates from network server 150 when needed (col. 20, lines 18-29). Waclawsky does not disclose or suggest, however, that data communications device 200 is an anonymous peer device or that data communications device 200 determines whether a received policy is the requested policy or discards the received policy when the received policy is not the requested policy, as required by claim 16.

For at least the foregoing reasons, Appellants submit that the rejection of claim 16 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

6. Claim 21.

Independent claim 21 is directed to a computer-readable medium containing instructions for controlling at least one processor to perform a method that distributes policies in a network having a policy server and a peer device. The method includes receiving one or more requests, where each request indicates a policy of interest to the peer device; determining whether an active version of each of the policies exists; and transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device recites receiving, via the anonymous peer device, a policy. Waclawsky does not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the combination of features recited in Appellants' claim 21. Therefore, the Examiner has not established a *prima facie* case of anticipation with respect to claim 21.

Nonetheless, Waclawsky does not disclose or suggest determining whether an active version of each of the policies exists and transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device. To the contrary, Waclawsky discloses that policy controller 250 in network devices 200 periodically obtains the latest version of network policy 207 from network policy server 150 (col. 20, lines 4-10).

Since Waclawsky does not disclose or suggest all of the features of claim 21, Waclawsky does not anticipate claim 21.

For at least the foregoing reasons, Appellants submit that the rejection of claim 21 under 35 U.S.C. § 102(e) based on Waclawsky is improper. Accordingly, Appellants request that the rejection be reversed.

B. Rejection under 35 U.S.C. § 103(a) based on Waclawsky (U.S. Patent No. 6,539,026) and McCloghrie et al. (U.S. Patent No. 6,286,052).

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the Examiner must provide a factual basis to support the conclusion of obviousness. In re Warner, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967). Based upon the objective evidence of record, the Examiner is required to make the factual inquiries mandated by Graham v. John Deere Co., 86 S.Ct. 684, 383 U.S. 1, 148 USPQ 459 (1966). The Examiner is also required to explain how and why one having ordinary

skill in the art would have been realistically motivated to modify an applied reference and/or combine applied references to arrive at the claimed invention. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988).

In establishing the requisite motivation, it has been consistently held that the requisite motivation to support the conclusion of obviousness is not an abstract concept, but must stem from the prior art as a whole to impel one having ordinary skill in the art to modify a reference or to combine references with a reasonable expectation of successfully achieving some particular realistic objective. See, for example, Interconnect Planning Corp. v. Feil, 227 USPQ 543 (Fed. Cir. 1985). Consistent legal precedent admonishes against the indiscriminate combination of prior art references. Carella v. Starlight Archery, 804 F.2d 135, 231 USPQ 644 (Fed. Cir. 1986); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985).

1. Claims 4, 8, 11, and 12.

With the above principles in mind, Appellants' claim 4 depends indirectly from claim 1. The disclosure of McCloghrie et al. does not remedy the deficiencies in the disclosure of Waclawsky set forth above with respect to claim 1. Therefore, claim 4 is patentable over Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1. Moreover, this claim is patentable over Waclawsky and McCloghrie et al. for reasons of its own.

Claim 4 recites storing, in response to a policy version becoming newly active, an identifier of the newly active policy in an active policy database, where the active policy database stores a list of active policy identifiers. The Examiner admits that Waclawsky does not disclose these features and relies on col. 14, lines 25-44, of McCloghrie et al. for allegedly

disclosing the features of claim 4 (final Office Action, pp. 4-6). Appellants submit that McCloghrie et al. does not disclose the features of claim 4.

At col. 14, lines 25-44, McCloghrie et al. discloses:

The first policy binding 552a, for example, may contain an encoded copy of the source port identified by program 224 with the SetSourcePort() call 414a and stored at the respective traffic flow data structure 234. More specifically, message generator 230 loads policy identifier field 562a with the type or instance of the policy element (e.g., "source port"). In the preferred embodiment, this name is a Policy Identifier (PID) as specified in the Internet Engineering Task Force (IETF) draft document COPS Usage for Differentiated Services submitted by the Network Working Group, dated December 1998, and incorporated herein by reference in its entirety. A PID specifies a particular policy class (e.g., a type of policy data item) or policy instance (e.g., a particular instance of a given policy class) in a hierarchical arrangement. The Policy ID type field 560a contains a predefined value reflecting that field 562a contains information in PID format. Component 226 preferably includes a Policy Information Base (PIB) for use in deriving the particular policy identifiers, as described in COPS Usage for Differentiated Services.

This section of McCloghrie et al. discloses placing a Policy Identifier (PID) in a message. This section of McCloghrie et al. does not disclose or suggest, however, storing a PID of a newly active policy in an active policy database, in response to a policy version becoming newly active, where the active policy database stores a list of active policy identifiers, as required by claim 4.

Even assuming, for the sake of argument, that one skilled in the art could reasonably construe the disclosure of McCloghrie et al. to disclose the features of claim 4, Appellants submit that one skilled in the art would not have been motivated to combine the teachings of Waclawsky and McCloghrie et al. in the manner suggested by the Examiner, absent impermissible hindsight. With respect to motivation, the Examiner alleges that "[i]t would have been obvious ... to combine the teachings of Waclawsky and McCloghrie to stores a list of active policy identifiers in an active policy database because it would allow a device to be

configured for a particular services using active policies stored in the active policy database" (final Office Action, pp. 4 and 6). Appellants disagree.

The Examiner has not pointed to any section of Waclawsky or McCloghrie et al. to support the Examiner's motivation to combine McCloghrie et al. with Waclawsky. Waclawsky does not disclose or suggest an active policy database. The Examiner's motivation falls short of logically explaining why one would seek to incorporate an active policy database into the Waclawsky system. The Examiner's motivation is merely conclusory and insufficient for establishing a *prima facie* case of obviousness.

For at least the foregoing reasons, Appellants submit that the rejection of claim 4 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

2. Claims 15 and 20.

Claim 15 depends indirectly from claim 13. The disclosure of McCloghrie et al. does not remedy the deficiencies in the disclosure of Waclawsky set forth above with respect to claim 13. Therefore, claim 15 is patentable over Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 13. Moreover, this claim is patentable over Waclawsky and McCloghrie et al. for reasons of its own.

Claim 15 recites that the determining, via the anonymous policy server, whether an active version of the policy exists includes comparing the identifier in the policy request to a list of active policy identifiers. Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, do not disclose or suggest this feature.

The Examiner has not addressed the feature recited in claim 15. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation,

Appellants' claims 1-4 do not recite comparing the identifier in the policy request to a list of active policy identifiers, as required by claim 15. Since the Examiner has not addressed the feature of claim 15, a *prima facie* case of obviousness has not been established with respect to claim 15.

For at least the foregoing reasons, Appellants submit that the rejection of claim 15 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

3. Claims 17-19.

Claim 17 is directed to network that includes at least one anonymous peer device and at least one anonymous policy server. The at least one anonymous peer device is configured to request a policy from at least one anonymous policy server, determine whether a received policy is of a desired policy class, and implement the received policy when the received policy is an active policy of the desired policy class. The at least one anonymous policy server is configured to receive the request from the at least one anonymous peer device, determine whether any version of the policy requested exists, and transfer all versions of the policy to the peer device, indicating the active version, if any version is determined to exist. Waclawsky and McCloghrie et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, Waclawsky and McCloghrie et al. do not disclose or suggest at least one anonymous peer device and at least one anonymous policy server. As set forth above, Waclawsky does not disclose or suggest that policy server 150 is an anonymous policy server. Moreover, Waclawsky does not disclose or suggest that network devices 200 are anonymous peer devices. McCloghrie et al. discloses a policy server 216, but does not disclose or suggest

that policy server 216 is an anonymous policy server. Moreover, McCloghrie et al. does not disclose or suggest at least one anonymous peer device.

As discussed above, the Examiner alleges that "Waclawsky did not discuss device authentication prior to obtain the updates. Therefore, the network policy server and the devices are anonymous" (final Office Action, pg. 5). Appellants disagree.

The mere fact that Waclawsky does not disclose device authentication in no way discloses or suggests that network policy server 150 and network devices 200 are anonymous. In fact, Waclawsky specifically discloses that network devices 200 are access servers, routers, switches, hubs, bridges, gateways, proxy servers, concentrators, repeaters, and similar data transfer devices (col. 7, lines 2-6). Such network devices are typically not anonymous since anonymity of these devices could hinder the transfer of data through communications network 100. For example, routers typically know the identity of other routers in proximity to themselves so as to know how to route data through a network. The Examiner has not pointed to any section of Waclawsky that supports the allegation that network policy server 150 and network devices 200 are anonymous.

Even assuming, for the sake of argument, that Waclawsky's network policy server 150 and network devices 200 could be considered anonymous, Waclawsky and McCloghrie et al. do not disclose features of Appellants' claim 17. For example, Waclawsky and McCloghrie et al. do not disclose or suggest at least one anonymous peer device that is configured to determine whether a received policy is of a desired policy class and implement the received policy when the received policy is an active policy of the desired policy class or at least one anonymous policy server that is configured to determine whether any version of a requested policy exists and transfer all versions of the policy to the peer device, indicating the active version if any version is determined to exist, as required by claim 17.

The Examiner has not addressed the features of claim 17. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above features of claim 17. Since the Examiner has not addressed the above features of claim 17, a *prima facie* case of obviousness has not been established with respect to claim 17.

For at least the foregoing reasons, Appellants submit that the rejection of claim 17 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

4. Claim 22.

Independent claim 22 recites a computer-readable medium having a database structure that includes a policy identification field that stores an identifier of a policy, a version field that stores an identifier of a policy version, and a policy content field that stores a content of a policy. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 22. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above features of claim 22. Since the Examiner has not addressed the above features of claim 22, a *prima facie* case of obviousness has not been established with respect to claim 22.

For at least the foregoing reasons, Appellants submit that the rejection of claim 22 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

5. Claim 23.

Independent claim 23 recites a computer-readable medium having a database structure that includes a policy identification field that stores an identifier of a policy, and a version field that stores an identifier of an active policy version. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 23. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above features of claim 23. Since the Examiner has not addressed the above features of claim 23, a *prima facie* case of obviousness has not been established with respect to claim 23.

For at least the foregoing reasons, Appellants submit that the rejection of claim 23 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

6. Claim 24.

Independent claim 24 is directed to a method for implementing policies. The method includes receiving a message, where the message contains an identifier and one or more versions of a policy; determining whether the identifier is in a list of policy identifiers; discarding the message when the identifier is absent from the list; and implementing an active version of the one or more policies when the identifier is present in the list. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 24. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above

combination of features of claim 24. Since the Examiner has not addressed the above features of claim 24, a *prima facie* case of obviousness has not been established with respect to claim 24.

For at least the foregoing reasons, Appellants submit that the rejection of claim 24 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

7. Claim 25.

Independent claim 25 is directed to a system for implementing policies. The system includes a memory and a processor. The memory is configured to store instructions and an active policy database, where the active policy database contains a list of policy identifiers. The processor is configured to execute the instructions to receive a message, where the message contains an identifier and one or more versions of a policy, compare the identifier to the list of policy identifiers, discard the message when the identifier does not match a policy identifier in the list, and implement an active version of the policy when the identifier matches a policy identifier in the list. Waclawsky and McCloghrie et al. do not disclose or suggest this combination of features.

Despite repeated requests by Appellants, the Examiner has not addressed the features recited in claim 25. Instead, the Examiner alleges that "[c]laims 5-25 have similar limitations as claims 1-4; therefore, they are rejected under the same rationale" (final Office Action, pg. 4). Contrary to the Examiner's allegation, Appellants' claims 1-4 do not recite the above combination of features of claim 25. Since the Examiner has not addressed the above features of claim 25, a *prima facie* case of obviousness has not been established with respect to claim 25.

For at least the foregoing reasons, Appellants submit that the rejection of claim 25 under 35 U.S.C. § 103(a) based on Waclawsky and McCloghrie et al. is improper. Accordingly, Appellants request that the rejection be reversed.

Application No.: 09/658207

Docket No.: BBNT-P01-109

VIII. CONCLUSION

In view of the foregoing arguments, Appellants respectfully solicit the Honorable Board to reverse the Examiner's rejections of claims 1-25 under 35 U.S.C. §§ 102 and 103.

Applicant believes no fee is due with this response other than as reflected on the enclosed fee transmittal. However, if a fee is due, please charge our Deposit Account No. 18-1945, under Order No. BBNT-P01-109 from which the undersigned is authorized to draw.

Dated: December 17, 2004

Respectfully submitted,

By 

Edward A. Gordon

Registration No.: 54,130

ROPES & GRAY LLP

One International Place

Boston, 02110-2624

(617) 951-7000

(617) 951-7050 (Fax)

Attorneys/Agents For Applicant

CLAIM APPENDIX

1. A method that ensures policy coherence among a group of peer devices, comprising:
 - detecting an addition of a new policy version;
 - generating a message containing the newly added policy version in response to detecting the addition of the new policy version; and
 - transferring the message to the peer devices.
2. The method of claim 1 wherein the newly added policy version is a policy that relates to at least one of system administration, system security, command and control, and courses of action.
3. The method of claim 1 further comprising:
 - determining whether a policy version has become newly active;
 - generating a second message containing an indication of the newly active policy version; and
 - sending the second message to the peer devices.
4. The method of claim 3 further comprising:
 - storing, in response to a policy version becoming newly active, an identifier of the newly active policy in an active policy database, the active policy database storing a list of active policy identifiers.

5. A system that ensures policy coherence among a group of peer devices, comprising:
- means for detecting an addition of one or more new policy versions;
 - means for generating a message containing the newly added one or more policy versions in response to detecting the addition of one or more policy versions; and
 - means for transferring the message to the peer devices.
6. A computer-readable medium containing instructions for controlling at least one processor to perform a method that ensures policy coherence among a group of peer devices, the method comprising:
- determining whether a policy has been added;
 - generating, in response to a policy being added, a message containing the added policy; and
 - sending the message to the peer devices.
7. The computer-readable medium of claim 6 wherein the method further comprises:
- determining whether a version of one of a group of policies has become active;
 - generating a second message containing the active version;
 - transferring the second message to the peer devices.
8. The computer-readable medium of claim 7 wherein the method further comprises:
- storing an identifier of the newly active policy in an active policy database, the active policy database including a list of active policy identifiers.

9. A policy server comprising:
 - a memory configured to store instructions; and
 - a processor configured to execute the instructions to determine whether one or more policy versions have been added, generate, in response to a policy version being added, a message containing the added policy version, and transfer the message to a group of peer devices.
10. The policy server of claim 9 wherein the processor is further configured to:
 - detect a policy version becoming newly active,
 - generate, in response to the detecting, a second message containing the newly active policy version, and
 - transmit the second message to the group of peer devices.
11. The policy server of claim 10 wherein the memory is further configured to:
 - store an active policy database containing a list of identifiers of active policies.
12. The policy server of claim 11 wherein the processor is further configured to:
 - store, in response to a policy becoming active, an identifier of the newly active policy in the active policy database.
13. A method for distributing policies in a network having at least one anonymous policy server and at least one anonymous peer device, comprising:
 - requesting a policy from the anonymous policy server;

determining, via the anonymous policy server, whether an active version of the policy exists; and

transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device.

14. The method of claim 13 wherein the requesting includes:

generating, via the anonymous peer device, a policy request, the policy request containing a policy identifier; and

transferring the policy request to the anonymous policy server.

15. The method of claim 14 wherein the determining includes:

comparing the identifier in the policy request to a list of active policy identifiers.

16. The method of claim 13 further comprising:

receiving, via the anonymous peer device, a policy;

determining whether the received policy is the requested policy;

discarding the received policy when the received policy is not the requested policy; and

implementing the received policy when the received policy is the requested policy.

17. A network comprising:

at least one anonymous peer device configured to:

request a policy from at least one anonymous policy server,

determine whether a received policy is of a desired policy class, and
implement the received policy when the received policy is an active
policy of the desired policy class; and
at least one anonymous policy server configured to:
receive the request from the at least one anonymous peer device,
determine whether any version of the policy requested exists, and
transfer all versions of the policy to the peer device, indicating the active
version, if any version is determined to exist.

18. The network of claim 17 wherein the at least one anonymous peer device is
further configured to:
discard the received policy when the received policy is not of the requested policy
class.

19. The network of claim 17 wherein, when requesting, the at least one anonymous
peer device is configured to:
generate a policy request, the policy request containing an identifier that identifies
the requested policy, and
transfer the policy request to the at least one anonymous policy server.

20. The network of claim 18 wherein, when determining, the at least one anonymous
policy server is configured to:
compare the identifier in the policy request to a list of active policy identifiers.

21. A computer-readable medium containing instructions for controlling at least one processor to perform a method that distributes policies in a network having a policy server and a peer device, the method comprising:

receiving one or more requests, each request indicating a policy of interest to the peer device;

determining whether an active version of each of the policies exists; and

transferring, when an active version of at least one of the policies exists, the at least one policy from the policy server to the peer device.

22. A computer-readable medium having a database structure comprising:

a policy identification field that stores an identifier of a policy;

a version field that stores an identifier of a policy version; and

a policy content field that stores a content of a policy.

23. A computer-readable medium having a database structure comprising:

a policy identification field that stores an identifier of a policy; and

a version field that stores an identifier of an active policy version.

24. A method for implementing policies, comprising:

receiving a message, the message containing an identifier and one or more versions of a policy;

determining whether the identifier is in a list of policy identifiers;

discarding the message when the identifier is absent from the list; and

implementing an active version of the one or more policies when the identifier is present in the list.

25. A system for implementing policies comprising:
 - a memory configured to store instructions and an active policy database, the active policy database containing a list of policy identifiers; and
 - a processor configured to execute the instructions to receive a message, the message containing an identifier and one or more versions of a policy, compare the identifier to the list of policy identifiers, discard the message when the identifier does not match a policy identifier in the list, and implement an active version of the policy when the identifier matches a policy identifier in the list.

Via: Express Mail EV 543609163 US Atty Dkt No.: BBNT-P01-109
Inventor: Donaghey et al.

Application No.: 09/658207 Filing Date: September 8, 2000
Title: SYSTEM AND METHOD FOR SELECTING AND DISSEMINATING POLICIES

Documents Filed:

Appeal Brief Transmittal (1 page)

Fee Transmittal (1 page)

Appeal Brief (32 pages)

Charge \$500.00 to deposit account 18-1945

Return postcard

Sender's Initials: EAG/dmc Date: December 17, 2004

9611640-1